View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by INRIA a CCSD electronic archive server

A simple presentation of the effective topos

Alexis Bernadet, Stéphane Graham-Lengrand

To cite this version:

Alexis Bernadet, Stéphane Graham-Lengrand. A simple presentation of the effective topos. [Research Report] LIX, Ecole polytechnique. 2012. hal-00844250

HAL Id: hal-00844250
https://hal.archives-ouvertes.fr/hal-00844250

Submitted on 14 Jul 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution - NonCommercial - ShareAlike| 4.0 International License

A simple presentation of the effective topos

Alexis Bernadet[1], Stéphane Graham-Lengrand[1,2]
[1]École Polytechnique, France
[2]CNRS, France

14th July 2013

Abstract

We propose for the Effective Topos an alternative construction: a realisability framework composed of two levels of abstraction.

This construction simplifies the proof that the Effective Topos is a topos (equipped with natural numbers), which is the main issue that this paper addresses. In this our work can be compared to Frey's monadic tripos-to-topos construction.

However, no topos theory or even category theory is here required for the construction of the framework itself, which provides a semantics for higher-order type theories, supporting extensional equalities and the axiom of unique choice.

1 Introduction

Topos Theory [Law64] can be used to abstract models of higher-order logic the same way Heyting algebras can be used for propositional logic. Contrary to set theories such as ZF, in Topos Theory, the expressions are typed.

A topos is a Cartesian closed category that satisfies certain properties. Even if the definition is simple, a topos describes an entire mathematical universe of high-order logic. The category of sets is a topos. So, when dealing with the internal logic of a topos, if we prove a result that is true in every topos, then this result is true in Set Theory. Therefore, the internal logic of a topos is not too "exotic".

In a topos, it is interesting to consider whether it has the following properties:

- The internal logic of the topos has the law of excluded middle
- Every morphism of the topos is "computable"
- The topos has *an object of natural integers* (definition of Lawvere)

With these three properties we can prove that the halting problem is computable which is absurd. Hence, a (non-degenerated) topos cannot have these three properties at the same time, so we have to use a different topos according to which high roder logic we want.

- If we have the first and the third properties, we have classical logic with arithmetics: the category of sets is such a topos.
- If we have the first and second properties but not the third one we have finite logic: the category of finite sets is such a topos.
- If we have the second and third properties but not the first one we have intuitionistic logic. There are several topos that satisfy these properties. One of the most famous ones is Hyland's effective topos [Hyl82, Pho92], which can be seen as the universe of realisability. Topos satisfying the second and third properties are the most interesting ones for computer science because they ensure that a programming language based on the Topos Theory can be given a constructive semantics.

In such a programming language, we can only write functions that terminate, as in proof assistants like Coq, so the language cannot be Turing-complete. The main advantage of having a programming language based on Topos Theory over more usual intuitionistic systems such as Martin-Loef type theory is the notion of equality: it is extensional, has proof-irrelevance, and allows the axiom of unique choice.

It is quite simple to check that the category of sets and the category of finite sets are topos. However, proving that the effective topos is indeed a topos is much harder [Hyl82]. This is mainly do to the fact that the notion of morphism in this category is not intuitive. The proof that the effective topos is a topos can be generalised with the Tripos Theory [Pit81], but this does not simplify the structure of the proof.

In this paper we present an alternative and simplier construction of a topos that turns out to be equivalent to Hyland's effective topos: This construction is based on a realisability framework with two levels of abstraction: a *low level*, comprising all the objects of the topos, and a *high level* used to define the morphisms.

Moreover, the high level

- identifies the properties that are needed to prove that the framework froms a topos, as simply as proving that the category of sets is a topos;
- can be directly used as a model of higher-order intuitionistic systems: Building such a semantics within the high level of the framework relies on the properties we prove to show that the full framework forms a topos.

This work can be compared to the monadic construction from Tripos to Topos [Fre11] but the constructions and properties of the framework does not require knowledge about category theory nor Topos Theory.

To our knowledge, the construction of this framework and this presentation of the effective Topos is new.

In Section 2, we define the core of the framework and prove its basic properties, especially how the results on the low level can be lifted to the high level. In Section 3, we give our own definition of an effective topos, we enrich the framework and prove that our effective topos is indeed a topos with an object of natural integers.

2 Presentation and general tools of the framework

In this section we are going to define the core and basic tools of our realisability framework. The main reason we choose to base our framework on realisability is to be able to do program extraction (see Theorem 29). In Section 2.1 we define the realisability part of the framework. In Section 2.2 we define the effective sets which will be the objects of the effective topos. In Section 2.3 we construct the high level part of the framework which is needed if we want the axiom of unique choice and the fact that the category that we construct is a topos (see Appendix B.3). In Section 2.4 we prove that a property that is true at the low level is also true at the high level, which is useful, because most of the properties we need for the framework are high-level properties. In Section 2.5 we define what a function in the framework is and how to build a high-level function from a low-level one. This is useful because most of the functions we need in our framework are high-level ones.

2.1 Realisability

Our framework is based on a notion of realisability that interprets formulae as sets of "proofs". As in Hyland's construction of the effective topos, we shall use integers to represent "proofs", but it could in fact be done with other well-known structures such as λ-terms.

Notation 1 If n and m integers, then we can code (n, m) by an integer and we write it $< n, m >$.

If e is an integer that codes a partial recursive function, then we write φ_e this function. And for all n, we write $\varphi_e(n)\downarrow$ if φ_e is defined in n and we write $\varphi_e(n)$ the image of n by φ_e.

- We write $\varphi_e(n)\downarrow= m$ for $\varphi_e(n)\downarrow$ and $\varphi_e(n) = m$.
- We write $\varphi_e(n)\downarrow\in F$ for $\varphi_e(n)\downarrow$ and $\varphi_e(n) \in F$

We write $Prop = P(\mathbb{N})$ with $\mathbb{N}$ the set of integers.

The definition of logical operators is inspired by Heyting semantics.

Definition 2 (Logical operators)
If $F, G \in Prop$ and $H \in X \to Prop$ with X a set, then we write:

$$\begin{array}{ll} \top & := \mathbb{N} \\ \bot & := \emptyset \\ F \wedge G & := \{< n, m >\mid n \in F\ m \in G\} \\ F \Rightarrow G & := \{e \mid \varphi_e\ exists \wedge \forall n \in F, \varphi_e(n)\downarrow\in G\} \\ \forall x \in X, H(x) & := \bigcap_{x\in X} H(x) \\ \exists x \in X, H(x) & := \bigcup_{x\in X} H(x) \end{array}$$

$F \Leftrightarrow G$ is an abbreviation for $(F \Rightarrow G) \wedge (G \Rightarrow F)$, and we write $\vDash F$ if and only if $F \neq \emptyset$.

Theorem 1 (Capturing intuitionistic provability)
The notion of inhabitation denoted $\vDash F$ with logic operators defined above admits the rules of deduction of intuitionistic first-order logic.

In the rest of the paper, we use this property implicitly to derive inhabitation results from simple intuitionist reasoning. For instance to prove $\vDash F \Rightarrow G$ we suppose F and then prove G: We admit that the reader can transform a intuitionistic first-order proof to an integer representing a program (via Curry-Howard). We can do this because there is no ambiguity between elements of $Prop$ and real mathematical formulae. The only theorems where we need to explicitly manipulate the integers as proofs are Lemma 26 and Theorem 29.

Remark 2 Had we chosen λ-terms to represent proofs, every result of the form $\vDash F$ that we prove in this paper would be such that F is inhabited by a λ-term typable in an extension of F_ω. [1]

2.2 Effective sets

The definition of effective sets is the same as the usual one [Hyl82]. It can be seen as a set with a partial equivalence relation (in the internal logic of the realisability).

Definition 3 (Effective sets) $X = (|X|, |. =_X .|)$ is an effective set if and only if :

- $|X|$ is a set.
- $|. =_X .| \in |X| \times |X| \to Prop$, and we write $|x =_X y|$ for $|. =_X .|(x, y)$.
- $\vDash \forall x, y \in |X|, |x =_X y| \Rightarrow |y =_X x|$ (Symmetry)
- $\vDash \forall x, y, z \in |X, |x =_X y| \Rightarrow |y =_X z| \Rightarrow |x =_X z|$ (Transitivity)

The main reason we do no require reflexivity in the definition is that a proof of $|x =_X x|$ may contain information. See Section 3.4 for example.

Remark 3 Assume X is an effective set. Then by symetry and transitivity we have
$\vDash \forall x, y \in |X|, |x =_X y| \Rightarrow (|x =_X x| \wedge |y =_X y|)$

Notation 4 (Quantification over an effective set)
Assume X is an effective set and $F \in |X| \to Prop$. We write:

- $\forall x \in X, F(x)$ for $\forall x \in |X|, |x =_X x| \Rightarrow F(x)$
- $\exists x \in X, F(x)$ for $\exists x \in |X|, |x =_X x| \wedge F(x)$.

This notation will shorten many properties and will make them more readable.

[1] We would need product sorts, and some notions of arithmetic -see the required notions in Section 3.

2.3 Elements

Contrary to the usual presentation of the effective topos, we use the notion of $El(X)$ as a core feature of the framework.

Definition 5 (Elements of an effective set)
If X is an effective set, we write $El(X)$ the effective set defined by:

$$\begin{array}{lcll} |El(X)| & := & |X| \to Prop & \\ |u =_{El(X)} v| & := & (\forall x, x' \in |X|, u(x) \Rightarrow |x =_X x'| \Rightarrow u(x')) & \text{(Stability)} \\ & \wedge & (\forall x, x' \in |X|, u(x) \Rightarrow u(x') \Rightarrow |x =_X x'|) & \text{(Unicity)} \\ & \wedge & (\exists x \in |X|, u(x)) & \text{(Existence)} \\ & \wedge & (\forall x \in |X|, u(x) \Leftrightarrow v(x)) & \text{(Equivalence)} \end{array}$$

It is straightforward to show that $El(X)$ is indeed an effective set.
$El(X)$ can be seen as the type of singletons included in X.

Remark 4 Assume X is an effective set. Then by uncity of u we have:
$\vDash \forall u, v \in |El(X)|, x \in |X|, |u =_{El(X)} v| \Rightarrow u(x) \Rightarrow |x =_X x|$

Manipulating $x \in |X|$ is considered low-level and manipulting $u \in |El(X)|$ without knowing that $|El(X)| = |X| \to Prop$ is considered high-level. With enough high-level theorems, it is possible to prove that the category we build is a topos by adapting the proof that the category of sets is a topos.

To achieve this we need a systematic way to lift structures and properties from the low level to the high level.

Definition 6 (Injection from the low level to the high level) If X is an effective set and $x \in |X|$, we define $el_X(x)$ as follows: For all, $y \in |X|$, $el_X(x)(y) := \ |x =_X y|$.

Lemma 5 (Basic relation between the low level and the high level)
If X is an effective set then:

1. $\vDash \forall u, v \in |El(X)|, |u =_{El(X)} u| \Rightarrow (\forall x \in |X|, u(x) \Leftrightarrow v(x)) \Rightarrow |u =_{El(X)} v|$
2. $\vDash \forall u, v \in El(X), (\forall x \in |X|, u(x) \Rightarrow v(x)) \Rightarrow |u =_{El(X)} v|$
3. $\vDash \forall u \in |El(X)|, |u =_{El(X)} el_X(x)| \Leftrightarrow (|u =_{El(X)} u| \wedge u(x))$
4. $\vDash \forall x, y \in |X|, |x =_X y| \Leftrightarrow |el_X(x) =_{El(X)} el_X(y)|$
5. $\vDash \forall u \in |El(X)|, |u =_{El(X)} u| \Leftrightarrow \exists x \in |X|, |u =_X el_X(x)|$

Proof:
Straightforward. See Appendix A.

□

2.4 Stable predicates

In this section we prove that properties that are true at the low-level are also true at the high-level. However, this is true only if the property is stable by equality. Hence we gave the following definition:

Definition 7 (Stable predicates) Assume X_1, …, X_n are effective sets.
A *stable predicate* on $(X_1, \ldots, X_n)$ is a $F \in (|X_1| \times \ldots |X_n|) \to Prop$ such that:

$$\vDash \forall x_1 \in |X_1|, \ldots, x_n \in |X_n|, x'_1 \in |X_1|, \ldots, x'_n \in |X_n|,$$
$$|x_1 =_{X_1} x'_1| \Rightarrow \ldots \Rightarrow |x_n =_{X_n} x'_n| \Rightarrow F(x_1, \ldots, x_n) \Rightarrow F(x'_1, \ldots, x'_n)$$

We write $SP(X_1, \ldots, X_n)$ the set of stable predicates on $(X_1, \ldots, X_n)$.

Generally, it is straightforward to prove that a property is stable because we only manipulate stable predicates and stable functions (see Section 2.5).

Then we can prove the main goal of this section. Notice that the lifting does not have to be on all the arguments of the predicate.

Theorem 6 (Extension of truth) *Assume $X_1, \ldots, X_n$ are effective sets, $k \leq n$, $F \in SP(El(X_1), \ldots, El(X_k), X_{k+1}, \ldots X_n)$ such that:*

$$\models \forall x_1 \in X_1, \ldots, x_n \in X_n, F(el_{X_1}(x_1), \ldots, el_{X_k}(x_k), x_{k+1}, \ldots x_n)$$

Then:

$$\models \forall u_1 \in El(X_1), \ldots, u_k \in El(X_k), x_{k+1} \in X_{k+1}, \ldots x_n \in X_n, F(u_1, \ldots, u_k, x_{k+1}, \ldots x_n)$$

Proof:

If $|u_1 =_{El(X_1)} u_1|, \ldots |u_k =_{El(X_k)} u_k|, |x_{k+1} =_{X_{k+1}} x_{k+1}|, \ldots |x_n =_{X_n} x_n|$, then by Lemma 5.5 there exist $x_1 \in |X_1|, \ldots, x_k \in |X_k|$ such that $|u_1 =_{El(X_1)} el_{X_1}(x_1)|, \ldots, |u_k =_{El(X_k)} el_{X_k}(x_k)|$. Then by symmetry we have $|el_{X_1}(x_1) =_{El(X_1)} u_1|, \ldots, |el_{X_k}(x_k) =_{El(X_k)} u_k|$. And by transitivity we have $|el_{X_1}(x_1) =_{El(X_1)} el_{X_1}(x_1)|, \ldots, |el_{X_k}(x_k) =_{El(X_k)} el_{X_k}(x_k)|$. So by Lemma 5.4 we have $|x_1 =_{X_1} x_1|, \ldots, |x_k =_{X_k} x_k|$. Hence by hypothesis we have $F(el_{X_1}(x_1), \ldots, el_{X_k}(x_k), x_{k+1}, \ldots x_n)$. And then by stability we have $F(u_1, \ldots, u_k, x_{k+1}, \ldots x_n)$.

□

With this theorem we can prove that if a proposition is true at the low level then it is true at the high level. We just have to check the stability of the proposition which is usually straightforward.

2.5 Stable functions

By manipulating effective sets, it is natural to be intersted in functions that are stable with the equality.

Definition 8 (Stable functions) Assume $X_1, \ldots, X_n$ and Y effective sets.

A *stable function* from $X_1, \ldots X_n$ to Y, is a $f \in (|X_1| \times \ldots |X_n|) \to |Y|$ such that:

$$\models \forall x_1 \in |X_1|, \ldots, x_n \in |X_n|, x'_1 \in |X_1|, \ldots, x'_n \in |X_n|,$$
$$|x_1 =_{X_1} x'_1| \Rightarrow \ldots \Rightarrow |x_n =_{X_n} x'_n| \Rightarrow |f(x_1, \ldots, x_n) =_Y f(x'_1, \ldots, x'_n)|$$

Such a stable function f is denoted $f : X_1 \to \ldots \to X_n \to Y$.

In this paper n will be equal to 1 or 2.

We will identify functions by extensionality.

Definition 9 (Equivalence of functions)

Assume X_1, ... X_n, and Y are effective sets, $f : X_1 \to \ldots X_n \to Y$ and $g : X_1 \to \ldots X_n \to Y$.

Then we write $f \approx g$ if and only if

$$\models \forall x_1 \in X_1, \ldots x_n \in X_n, |f(x_1, \ldots, x_n) =_Y g(x_1, \ldots, x_n)|$$

It is straightforward that $\approx$ is an equivalence relation.

With the following theorem we are able to write high level functions by using low level ones.

Definition 10 (Extension of function)

Assume X_1, ... X_n, and Y effective sets, $f : X_1 \to \ldots X_n \to El(Y)$ and $k \leq n$.

An *extension* of f on the first k arguments is a $g : El(X_1) \to \ldots El(X_k) \to X_{k+1} \to \ldots X_n \to El(Y)$ such that:

$$\models \forall x_1 \in X_1, ...x_n \in X_n, |g(el_{X_1}(x_1), ..., el_{X_k}(x_k), x_{k+1}, \ldots, x_n) =_{El(Y)} f(x_1, ..., x_n)|$$

Theorem 7 (Existence and unicity of extensions of functions)

Assume X_1, ... X_n, and Y effective sets, $f : X_1 \to \ldots X_n \to El(Y)$ and $k \leq n$.

We construct $g \in (|El(X_1)| \times ... \times |El(X_k)| \times |X_{k+1}| \times ... \times |X_n|) \to |El(Y)|$ defined by:

$$g(u_1, \ldots, u_k, x_{k+1} \ldots x_n)(y) := \quad \exists x_1 \in |X_1|, ..., x_k \in |X_k|, \\ u_1(x_1) \wedge ... \wedge u_k(x_k) \wedge f(x_1, ..., x_n)(y)$$

Then:

- *g is an extension of f on the first k arguments.*
- *For all h extension of f on the first k arguments we have $h \approx g$*

Proof:

For readability we are only going to prove the case where $n = k = 1$ and $X = X_1$. This proof can easily be adapted to the case with several arguments and where the extension is not necessarily on all the arguments. See proof in Appendix A for the general case which works for any values of k and n.

- First we prove that $g : El(X) \to El(Y)$ which means proving stability of g. If $|u =_{El(X)} u'|$: We want to prove that $|g(u) =_{El(Y)} g(u')|$.
  - If $g(u)(y)$ and $|y =_Y y'|$ then by definition of g, there exists $x \in |X|$, such that $u(x)$ and $f(x)(y)$. Then because $|u =_{El(X)} u'|$ we have $|x =_X x|$ by using unicity of u. Hence, $|f(x) =_{El(Y)} f(x)|$ by stability of f. So, $f(x)(y')$ by stability of $f(x)$. Hence, we have $g(u)(y')$.
  - If $g(u)(y)$ and $g(u)(y')$ then by definition of g, there exists x and x' in $|X|$ such that $u(x)$, $u(x')$, $f(x)(y)$ and $f(x')(y')$. Because $|u =_{El(X)} u'|$ we have $|x =_X x'|$ by unicity of u. Hence $|f(x) =_{El(Y)} f(x')|$ by stability of f. So we have $f(x)(y')$ by equivalence between $f(x)$ and $f(x')$. And then $|y =_Y y'|$ by unicity of $f(x)$.
  - $|u =_{El(X)} u'|$, so there exists $x \in |X|$ such that $u(x)$. Then we have $|x =_X x|$ by unicity of u. Hence $|f(x) =_{El(Y)} f(x)|$ by stability of f. So there exists $y \in |Y|$, such that $f(x)(y)$. Then we have $g(u)(y)$ by definition of g. Hence there exists $y \in |Y|$ such that $g(u)(y)$.
  - If $g(u)(y)$ then there exists $x \in |X|$, such that $u(x)$ and $f(x)(y)$. So we have $u'(x)$. Hence we have $g(u')(y)$.
  - By a similar argument, if $g(u')(y)$ then $g(u)(y)$.

  Hence $|g(u) =_{El(Y)} g(u')|$. Therefore $g : El(X) \to El(Y)$.

- If $|x =_X x|$:
  - Then $|f(x) =_{El(Y)} f(x)|$, $|el_X(x) =_{El(X)} el_X(x)|$ (from Lemma 5.4) and $|g(el_X(x)) =_{El(Y)} g(el_X(x))|$
  - If $g(el_X(x))(y)$ then there exists $x' \in |X|$ such that $el_X(x)(x')$ and $f(x')(y)$. Hence $|x =_X x'|$. So we have $|f(x) =_{El(Y)} f(x')|$. Hence we have $f(x)(y)$.

  Hence we have $|g(el_X(x)) =_{El(Y)} f(x)|$ by Lemma 5.2. Therefore, g is an extension of f.

- If h is an extension of f. We construct $F \in |El(X)| \to Prop$ defined by $F(u) := |g(u) =_{El(Y)} h(u)|$. By stability of g and h we have $F \in SP(X)$.

  If $|x =_X x|$, then, because g and h are extensions of f we have $|g(el_X(x)) =_{El(Y)} f(x)|$ and $|h(el_X(x)) =_{El(Y)} f(x)|$. Hence we have $|g(el_X(x)) =_{El(Y)} h(el_X(x))|$ which is $F(el_X(x))$.

  By Theorem 6, we can prove that $\vDash \forall u \in El(X), F(u)$.

  Therefore, $g \approx h$ by definition of F and $\approx$.

□

3 The Effective Topos

In this section we construct a category that we call *The effective Topos*. To prove that this category is a topos with an object of natural integers, we prove results in the high level part of our framework. Except for the axiom of unique choice, these results are extensions from the low level to the high level. We also prove that we can do program extraction in the framework. The fact that our definition of the Effective Topos is equivalent Hyland's is given in Appendix B.2. We say that we *extend* the framework if we define new operators and prove new properties in this framework. In section 3.1 we construct the Effective Topos. In section 3.2 we extend the framework to prove that this category is Cartesian closed. In section 3.3 we extend the framework to prove that this category has a sub-object classifier (therefore it is a topos). In section 3.4 we extend the framework to prove that this category has an object of natural integers and we also prove that we can do program extraction with our framework.

3.1 Definition of the category

To build the category we must first check that the composition is well-defined for functions of this framework.

Lemma 8 (Correctness of composition) *Assume X, Y and Z are effective sets:*

- *If $f : X \to Y$ and $g : Y \to Z$, then $g \circ f : X \to Z$.*
- *If $f : X \to Y$, $f' : X \to Y$, $g : Y \to Z$, $g' : Y \to Z$, $f \approx f'$ and $g \approx g'$, then $g \circ f \approx g' \circ f'$.*

Proof: Straightforward. See Appendix A. □

Theorem 9 (Definition of the category C) *We build $\boldsymbol{C}$ the category whose objects are the effective sets and the morphisms between two objects X and Y are the functions $f : El(X) \to El(Y)$ modulo the $\approx$ relation. And the composition is the usual composition.*

It is straightforward that $\boldsymbol{C}$ is a category (the identity is the usual identity).

We call this category the effective topos. We will prove (in Appendix B.2) that this definition is equivalent to the usual definition by Hyland.

3.2 This category is Cartesian closed

A Cartesian closed category is a category that has a final object, products, and power objects (closure over the product).

3.2.1 Final object

Let S be a set and $()$ an element of S.

Definition 11 (Definition of 1) We build 1 the effective set defined by:

- $|1| := S$
- $|x =_1 y| := \top$

It is straightforward that 1 is an effective set.

Here is the high level constant (defined with the low level one):

Definition 12 (Definition of $<>$) We define $<> \in |El(1)|$ by $<> := el_1(())$.

Here are the high level properties we need to prove that **C** has a final object.

Theorem 10 (Properties of 1)

- $\models | <> =_1 <> |$
- $\models \forall u, v \in El(1), |u =_1 v|$

Proof:

Straightforward. To prove the second item, we use Theorem 6. See Appendix A.

□

Now with the previous theorem we can easily prove the categorical result:

Theorem 11 (C has a final object) *1 is the final object of* $\mathbf{C}$.

Proof: Corollary of Theorem 10. See Appendix A. □

3.2.2 Product

To prove that $\mathbf{C}$ has products we use the same method as in Section 3.2.1.

This is the minimum requirement to prove that $\mathbf{C}$ has products:

If X and Y sets, then $X \times Y$ is a set. If $z \in X \times Y$, then $\pi_1(z) \in X$ and $\pi_2(z) \in Y$. And if $x \in X$ and $y \in Y$, then $(x, y) \in X \times Y$, $\pi_1(x, y) = x$ and $\pi_2(x, y) = y$.

The definition of the product is the same as the one in the usual presentation of the effective topos.

Definition 13 (Definition of $A \times B$) If A and B effective sets, then we define $A \times B$ by:

- $|A \times B| := |A| \times |B|$
- $|c =_{A \times B} c'| := |\pi_1(c) =_A \pi_1(c')| \wedge |\pi_2(c) =_B \pi_2(c')|$

It is trivial to show that $A \times B$ is an effective set.

For the high level operators it will be less trivial than in the case of the final object: we define the high level constructions by using Theorem 7.

Definition 14 (Definition of p'_1, p'_2 and $cons'$) We construct $p'_1 \in |A \times B| \to |El(A)|$, $p'_2 \in |A \times B| \to |El(B)|$ and $cons' \in (|A| \times |B|) \to |El(A \times B)|$ as follows:
$p'_1(c) := el_A(\pi_1(c))$, $p'_2(c) := el_B(\pi_2(c))$, $cons'(a, b) := el_{A \times B}((a, b))$

Lemma 12 (Stability of p'_1, p'_2 and $cons'$)
$p'_1 : (A \times B) \to El(A)$, $p'_2 : (A \times B) \to El(B)$ *and* $cons' : A \to B \to El(A \times B)$.

Proof: Straightforward. See Appendix A. □

Definition 15 (Definition of p_1, p_2 and $< u, v >$) Assume A and B are effective sets.

- We write $p_1 : El(A \times B) \to El(A)$ the extension of p'_1.
- We write $p_2 : El(A \times B) \to El(B)$ the extension of p'_2.
- We write $cons : El(A) \to El(B) \to El(A \times B)$ the extension of $cons'$.
  We write $< u, v >$ for $cons(u, v)$.

The high level constructions satisfy stability, β-equivalence, and extensionality:

Theorem 13 (Properties of $A \times B$)
Assume A and B are effective sets.

- $\models \forall w, w' \in |El(A \times B)|, |w =_{El(A \times B)} w'| \Rightarrow |p_1(w) =_{El(A)} p_1(w')|$
- $\models \forall w, w' \in |El(A \times B)|, |w =_{El(A \times B)} w'| \Rightarrow |p_2(w) =_{El(B)} p_2(w')|$
- $\models \forall u, u' \in |El(A)|, v, v' \in |El(B)|,$
  $|u =_{El(A)} u'| \Rightarrow |v =_{El(B)} v'| \Rightarrow |< u, v > =_{El(A \times B)} < u', v' >|$
- $\models \forall u \in El(A), v \in El(B), |p_1(< u, v >) =_{El(A)} u|$
- $\models \forall u \in El(A), v \in El(B), |p_2(< u, v >) =_{El(B)} v|$
- $\models \forall w, w' \in El(A \times B), |p_1(w) =_{El(A)} p_1(w')| \Rightarrow |p_2(w) =_{El(B)} p_2(w')| \Rightarrow |w =_{El(A \times B)} w'|$

Proof: Straightforward with the use Theorem 6 and the definitions of p_1, p_2 and $cons$. See Appendix A. □

With this theorem we can conclude the categorical result:

Theorem 14 (C has products)
If A and B effective sets, then $A \times B$ is the product of A and B in $\boldsymbol{C}$, p_1 and p_2, its projections. Hence $\boldsymbol{C}$ is cartesian.

Proof: Corollary of Theorem 13. See Appendix A. □

3.2.3 Closure

Compared to Heyting's, because we do not have the same notion of morphisms, the definition of the power object is not the same: it is much simpler.

Definition 16 (Definition of $A \Rrightarrow B$)
Assume A and B are effective sets. Then we define the effective set $A \Rrightarrow B$ as follows:

- $|A \Rrightarrow B| := \ |El(A)| \to |El(B)|$
- $|f =_{A \Rrightarrow B} g| := \ (\forall u, u' \in |El(A)|, |u =_{El(A)} u'| \Rightarrow |f(u) =_{El(B)} g(u')|)$

It is straightforward to prove that $A \Rrightarrow B$ is an effective set.

$|f =_{A \Rrightarrow B} g|$ is equivalent to expressing internaly that: f is stable, g is stable and f and g are equivalent.

As in the product case, we define high level constructors and destructors.

Definition 17 (Definition of app')
We construct $app' \in (|A \Rrightarrow B| \times |El(A)|) \to |El(B)|$ defined by: $app'(f, u) := \ f(u)$

Lemma 15 (Stability of app') $app' : (A \Rrightarrow B) \to El(A) \to El(B)$

Proof: Straightforward. See Appendix A. □

Definition 18 (Definition of app and $\Lambda u : A.f(u)$) Assume A and B are effective sets.

- We write $app : El(A \Rrightarrow B) \to El(A) \to El(B)$ the extension of app' on the first argument.
- If $f \in |El(A)| \to |El(B)|$ we write $\Lambda u : A.f(u)$ for $el_{A \Rrightarrow B}(u \in |El(A)| \mapsto f(u))$.

And as in the product case, we can prove stability, β-equivalence and extensionality on these high level operators.

Theorem 16 (Properties of $A \Rrightarrow B$) *Assume A and B are effective sets.*

- $\models \forall w, w' \in |El(A \Rrightarrow B)|, u, u' \in |El(A)|,$
  $|w =_{El(A)} w'| \Rightarrow |u =_{El(A)} u'| \Rightarrow |app(w, u) =_{El(B)} app(w', u')|$
- $\models \forall f, f' \in |El(A)| \to |El(B)|, (\forall u, u' \in |El(A)|,$
  $|u =_{El(A)} u'| \Rightarrow |f(u) =_{El(B)} f'(u')|) \Rightarrow |\Lambda u : A.f(u) =_{El(A \Rrightarrow B)} \Lambda u : A.f'(u)|$
- $\models \forall f \in |El(A)| \to |El(B)|, u \in El(A),$
  $(\forall v, v' \in |El(A)|, |v =_{El(A)} v'| \Rightarrow |f(v) =_{El(B)} f(v')|)$
  $\Rightarrow |app((\Lambda v : A.f(v)), u) =_{El(B)} f(u)|$
- $\models \forall w, w' \in El(A \Rrightarrow B), (\forall u \in El(A), |app(w, u) =_{El(B)} app(w', u)|) \Rightarrow |w =_{El(A \Rrightarrow B)} w'|$

Proof: Only the last point is not trivial and it can be proven by using Theorem 6. See Appendix A. □

And then we can prove this theorem as easy as in the case of the category of sets.

Theorem 17 (C has power objects) *If A and B effective sets then $A \Rrightarrow B$ with $ev : El((A \Rrightarrow B) \times A) \rightarrow El(B)$ defined by $ev(w) :=\ app(p_1(w), p_2(w))$ is B power A in $\boldsymbol{C}$.*

Hence $\boldsymbol{C}$ is cartesian and closed.

Proof: Corollary of Theorem 16. See Appendix A. □

3.3 The sub-object classifier

To prove that **C** is a topos, we only have to prove that **C** has a sub-object classifier (which can be seen as the object of truth values).

There are several possible definition of the sub-object classifier. The one we use here needs the notion of pullback and monomorphism which can be used as the categorical definition of subset and defined as follows in **C**:

Definition 19 (Pullback of a morphism from the final object)

Assume X is an effective set.

By Theorem 11 we can construct $* : El(X) \rightarrow El(1)$ defined by $*(u) := <>$.

Assume A and Ω are effective sets, $True : El(1) \rightarrow El(\Omega)$ and $f : El(A) \rightarrow El(\Omega)$.

Then i is the *pullback of $True$* along f if and only if:

- B is an effective set and $i : El(B) \rightarrow El(A)$.
- $f \circ i \approx True \circ *$.
- For all effective set X and for all $\varphi : El(X) \rightarrow El(A)$, if $f \circ \varphi \approx True \circ *$ then there exists a unique $\psi : El(X) \rightarrow El(A)$ (modulo $\approx$) such that $i \circ \psi \approx \varphi$.

B can be seen as the categorical definition of the subset of A which elements satisfies f and with i the injection morphism.

Definition 20 (Monomorphism)

Assume A and B are effective sets and $m : El(A) \rightarrow El(B)$.

m is a *monomorphism* if and only if for all effective sets X and for all $f, g : El(X) \rightarrow El(A)$, if $m \circ f \approx m \circ g$ then $f \approx g$.

This can be seen as the categorical definition of injectivity.

Now we can give the definition of a sub-object classifier:

Definition 21 (Sub-object classifier) Ω with $True$ is a *sub-object-classifier* if and only if:

- Ω is an effective set and $True : El(1) \rightarrow El(\Omega)$.
- For all effective sets A and for all $f : El(A) \rightarrow El(\Omega)$ there exists a pullback of $True$ along f.
- For all effective sets A and B and for all $m : El(A) \rightarrow El(B)$ monomorphism there exists a unique $\chi_m : El(B) \rightarrow El(\Omega)$ (modulo $\approx$) such that m is the pullback of $True$ along χ_m.

As in the case of the final object, the products and the power objects, the sub-object classifier is unique up to isomorphism.

3.3.1 Propositions

In this section we construct Ω and $True$ and we characterize the property that $f \approx True \circ *$ for some $f : El(X) \to El(\Omega)$.

The construction of the sub-object classifier is the same as in Heyting's.

Definition 22 (Definition of Ω) We define the effective set Ω as follows:

- $|\Omega| := \ Prop$
- $|q =_\Omega q'| := \ q \Leftrightarrow q'$

It is trivial to prove that Ω is an effective set.

Unlike the general case, Ω is an effective set where it is possible to go directly from the high level to the low level.

Definition 23 (Definition of prop) If $u \in El(Prop)$ we write $prop(u) := \ u(\top)$

And $prop$ is the opposite of el_Ω as follows:

Theorem 18 (Properties of Ω)

- $\models \forall q, q' \in Prop, (q \Leftrightarrow q') \Leftrightarrow |el_\Omega(q) =_{El(\Omega)} el_\Omega(q')|$
- $\models \forall u, v \in |El(\Omega)|, |u =_{El(\Omega)} v| \Rightarrow (prop(u) \Leftrightarrow prop(v))$
- $\models \forall q \in Prop, prop(el_\Omega(q)) \Leftrightarrow q$
- $\models \forall u, v \in El(\Omega), (prop(u) \Leftrightarrow prop(v)) \Rightarrow |u =_{El(\Omega)} v|$

Proof: Straightforward. See Appendix A. □

Then we can connect the categorical world and the framework for the notion of truth as follows:

Definition 24 (Definition of $True$)
We construct $True \in |El(1)| \to |El(\Omega)|$ and defined by: $True(u) := \ el_\Omega(\top)$

Theorem 19 (Properties of $True$) *We have $True : El(1) \to El(\Omega)$.*
Furthermore, assume that X is an effective set.
Then for all $f : El(X) \to El(\Omega)$, $f \approx True \circ *$ if and only if $\models \forall u \in El(X), prop(f(u))$

Proof: Corollary of Theorem 18. See Appendix A. □

If $f : El(X) \to El(\Omega)$ then the property $f \approx True \circ *$ is often used in the characterisation of the sub-object classifier in the topos theory.

3.3.2 Subsets

In this section, we prove that there exist pullbacks of $True$.

The construction of subsets in this framework is quite intuitive: first we define the effective object that represent a subset, then we prove the main property in the high level framework, and finally we prove that it respects the categorical characterisation.

Definition 25 (Definition of $\{u \in A \mid F(u)\}$) Assume A is an effective set and $F \in SP(El(A))$. We define the effective set $\{u \in A \mid F(u)\}$ as follow:

- $|\{u \in A \mid F(u)\}| := \ |A|$
- $|x =_{\{u \in A|F(u)\}} y| := \ |x =_A y| \wedge F(el_A(x))$

It is trivial to show that $\{u \in A \mid F(u)\}$ is an effective set.

Theorem 20 (Properties of $\{u \in A \mid F(u)\}$)
Assume A is an effective set and $F \in SP(El(A))$. Let $B := \ \{u \in A|F(u)\}$. Then:
$\models \forall u, v \in |El(A)|, |u =_{El(B)} v| \Leftrightarrow (|u =_{El(A)} v| \wedge F(u))$

Proof: Straightforward. See Appendix A. □

Theorem 21 (C has pullbacks of $True$) *Assume A is an effective set and $f : El(A) \to El(\Omega)$. Then B defined by $B := \{u \in A \mid prop(f(u))\}$ is an effective set and if $i(u) := u$ then $i : El(B) \to El(A)$ and B with i is the pullback of $True$ along f.*

Proof: Corollary of Theorem 20. See Appendix A. □

3.3.3 Monomorphisms

We use a definition of the sub-object classifier that uses monomorphisms. So it is useful to have a relation between the notion of monomorphisms and the notion of injectivity (as in the category of sets) defined in the high level of the framework as follows:

Definition 26 (Injective) Assume A and B effective sets and $f : El(A) \to El(B)$.
We say that f is injective if and only if:
$\models \forall u, u' \in El(A), |f(u) =_{El(B)} f(u')| \Rightarrow |u =_{El(A)} u'|$

Theorem 22 (Equivalence between monorphisms and injective functions)
Assume A and B effective sets and $m : El(A) \to El(B)$.
*m is a monomorphism in **C** if and only if m is injective.*

Proof:
Straightforward: We adapt the proof of the category of sets. See Appendix A. □

We can notice that, to prove this theorem, we did not had to add any new construction to the framework.

3.3.4 Axiom of unique choice

In this section we construct χ_m.

One of the advantages of this framework as a model of high order logic is to have the axiom of unique choice.

To express it we first define the operator of description:

Definition 27 (Operator of description)
Assume A is an effective set and $F \in |El(A)| \to Prop$ (i.e. $F \in |El(El(A))|$).
We construct $d(F) \in |El(A)|$ defined by: for all $x \in |A|$, $d(F)(x) := F(el_A(x))$.
$d(F)$ can be read as "the only u such that $F(u)$".

Before proving the axiom of unique choice:

Theorem 23 (Properties of $d(F)$) *Assume A is an effective set and then:*
$\models \forall F \in El(El(A)), F(d(F))$ *which is equivalent to:*

$$\begin{aligned} \models \forall F \in |El(A)| \to Prop, \\ &(\forall u, u' \in |El(A)|, F(u) \Rightarrow |u =_{El(A)} u'| \Rightarrow F(u')) \\ &\Rightarrow (\forall u, u' \in |El(A)|, F(u) \Rightarrow F(u') \Rightarrow |u =_{El(A)} u'|) \\ &\Rightarrow (\exists u \in |El(A)|, F(u)) \\ &\Rightarrow F(d(F)) \end{aligned}$$

Proof:
Assume we have

- $\forall u, u' \in |El(A)|, F(u) \Rightarrow |u =_{El(A)} u'| \Rightarrow F(u')$,
- $\forall u, u' \in |El(A)|, F(u) \Rightarrow F(u') \Rightarrow |u =_{El(A)} u'|$, and
- $\exists u \in |El(A)|, F(u)$.

So there exists $u \in |El(A)|$ such that $F(u)$. By unicity of F (with $u' = u$), $|u =_{El(A)} u|$.

- If $u(a)$ then by Lemma 5.3 we have $|u =_{El(A)} el_A(a)|$. By stability of F, $F(el_A(a))$. Therefore $d(F)(a)$ by definition of $d(F)$.
- If $d(F)(a)$, then by definition of $d(F)$ we have $F(el_A(a))$. By unicity of F, $|u =_{El(A)} el_A(a)|$. By Lemma 5.3, we have $u(a)$.

By Lemma 5.1, $|u =_{El(A)} d(F)|$. Therefore, by stability of F, we have $F(d(F))$. □

Theorem 23 is necessary to prove the last hypothesis needed to have a topos.

Definition 28 (Caracteristic morphism)
Assume A and B is effective sets, and $m : El(A) \to El(B)$ a monomorphism.
Then with define $\chi_m \in |El(B)| \to |El(\Omega)|$ defined by: $\chi_m(v) := \; el_\Omega(\exists u \in El(A), |m(u) =_{El(B)} v|)$

Theorem 24 (Monomorphisms of C have a caracteristic morphism)
Assume A and B is effective sets, and $m : El(A) \to El(B)$ a monomorphism.
Then we have $\chi_m : El(B) \to El(\Omega)$.
And it is the only morphism (modulo $\approx$) from B to Ω in $\boldsymbol{C}$ such that m is the pullback of $True$ along χ_m.

Proof: We adapt the proof of the category of sets. See Appendix A.
In particular, from a $\varphi : El(X) \to El(B)$ such that $\chi_m \circ \varphi \approx True \circ *$ we use Theorem 23 to construct $\psi : El(X) \to El(A)$. □

By combining all the categorical results of this part we can finally conclude.

Theorem 25 *$\boldsymbol{C}$ is a topos and Ω with $True$ is the sub-object classsifier.*

Proof:
By Theorem 17, C is Cartesian Closed. By Theorems 21 and 24, Ω with $True$ is the sub-object classifier in **C** Hence **C** is a topos.

□

3.4 Natural numbers

The main advantage of the effective topos over the category of finite sets is that it has an object of natural integers.

Let $\mathbb{N}$ be the set of natural integers, with $0 \in \mathbb{N}$ and $s \in \mathbb{N} \to \mathbb{N}$ the successor function.

Definition 29 (Equality in $\mathbb{N}$) We construct $E \in (\mathbb{N} \times \mathbb{N}) \to Prop$ defined by:

$$\begin{array}{lcll} E(n,n) & = & \{n\} & \\ E(n,m) & = & \emptyset & n \neq m \end{array}$$

Lemma 26 (Properties of E)

1. $\vDash E(0,0)$
2. $\vDash \forall x, y \in \mathbb{N}, E(x,y) \Rightarrow E(s(x), s(y))$
3. $\vDash \forall x, y \in \mathbb{N}, E(x,y) \Rightarrow E(y,x)$
4. $\vDash \forall x, y, z \in \mathbb{N}, E(x,y) \Rightarrow E(y,z) \Rightarrow E(x,z)$
5. $\vDash \forall x, y \in \mathbb{N}, E(s(x), s(y)) \Rightarrow E(x,y)$
6. $\vDash \forall x \in \mathbb{N}, E(s(x), 0) \Rightarrow \bot$
7. *For all* $\vDash \forall P \in \mathbb{N} \to Prop, P(0) \Rightarrow (\forall x \in \mathbb{N}, P(x) \Rightarrow P(s(x))) \Rightarrow$
   $\forall x \in \mathbb{N}, E(x,x) \Rightarrow P(x)$

Proof: Straightforward but we have to explicitly manipulates proofs as programs. See Appendix A. □

These properties are useful if we want to adapt this work with an extension of system F_ω.

Definition 30 (Effective set of natural integers) We define the effective set Nat as follows:

- $|Nat| := \mathbb{N}$
- $|x =_{Nat} y| := E(x, y)$

By Lemma 26, we can prove that Nat is an effective set.

We naturally have the high level constructions as a lift of the low level ones.

Definition 31 (Definition of Z and S) We define $Z \in |El(Nat)|$ and $S' \in |Nat| \to |El(Nat)|$ as follow: $Z := el_{Nat}(0)$ and $S'(x) := el_{Nat}(s(x))$.

By Lemma 26.2, we have $S' : Nat \to El(Nat)$.

We write $S : El(Nat) \to El(Nat)$ the extension of S'.

We can then prove the stability and the axioms of Peano in the high level of the framework.

Theorem 27 (Properties of Nat)

- $\models |Z =_{El(Nat)} Z|$
- $\models \forall u, v \in |El(Nat)|, |u =_{El(Nat)} v| \Rightarrow |S(u) =_{El(Nat)} S(v)|$
- $\models \forall u, v \in El(Nat), |S(u) =_{El(Nat)} S(v)| \Rightarrow |u =_{El(Nat)} v|$
- $\models \forall u \in El(Nat), |S(u) =_{El(Nat)} Z| \Rightarrow \bot$
- *For all* $P \in SP(El(Nat))$,
  if $\models P(Z)$ *and* $\models \forall u \in El(Nat), P(u) \Rightarrow P(S(u))$ *then* $\models \forall u \in El(Nat), P(u)$

Proof: Straightforward with Lemma 26 and Theorem 6. See Appendix A □

Finally we can conclude than **C** has an object of natural integers:

Theorem 28 (C has an object of integers) *We construct $Z_m \in |El(1)| \to |El(Nat)|$ defined by $Z_m(u) := Z$. (Nat, Z_m, S) is the object of natural integers in the category **C** which means that:*

- $Z_m : El(1) \to El(Nat)$ *and* $S : El(Nat) \to El(Nat)$
- *For all X effective set, $f : El(1) \to El(X)$, $g : El(X) \to El(X)$, there exists a unique (modulo $\approx$) $\varphi : El(Nat) \to El(X)$ such that $\varphi \circ Z_m \approx f$ and $\varphi \circ S \approx g \circ \varphi$*

Proof:

With Theorem 27, we can prove that (Nat, Z_m, S) satisfies the Peano axioms in the internal logic of the topos **C**. Therefore, (Nat, Z_m, S) is the object of naturals integers in **C**.

□

Because our framework is based on realisability, we can do program extraction:

Theorem 29 (Program extraction) *Assume $f : El(Nat) \to El(Nat)$.*

There exists a unique $g \in \mathbb{N} \to \mathbb{N}$ such that:

$$\models \forall x \in Nat, |f(el_{Nat}(x)) =_{El(Nat)} el_{Nat}(g(x))|$$

And then, g is computable.

Proof:

If $E(x, x)$ then $|el_{Nat}(x) =_{El(Nat)} el_{Nat}(x)|$. So, $|f(el_{Nat}(x)) =_{El(Nat)} f(el_{Nat}(x))|$. Hence, there exists $m \in |Nat|$, such that $|f(el_{Nat}(x)) =_{El(Nat)} el_{Nat}(m)|$.

Therefore, $\models \forall x \in \mathbb{N}, E(x, x) \Rightarrow \exists m \in N, |f(el_{Nat}(x)) =_{El(Nat)} el_{Nat}(m)|$.

Hence, there exists $e \in \forall x \in \mathbb{N}, E(x, x) \Rightarrow \exists m \in \mathbb{N}, |f(el_{Nat}(x)) =_{El(Nat)} el_{Nat}(m)|$. Then φ_e exists. Let $x \in \mathbb{N}$. So $x \in E(x, x)$. Hence $\varphi_e(x) \downarrow \in \exists m \in \mathbb{N}, |f(el_{Nat}(x)) =_{El(Nat)} el_{Nat}(m)|$.

Therefore, there exists $m \in \mathbb{N}$ such that $\varphi_e(x) \in |f(el_{Nat}(x)) =_{El(Nat)} el_{Nat}(m)|$. Let $m' \in \mathbb{N}$ such that $\varphi_e(x) \in |f(el_{Nat}(x)) =_{El(Nat)} el_{Nat}(m')|$. Hence $\vDash |f(el_{Nat}(x)) =_{El(Nat)} el_{Nat}(m)|$ and $\vDash |f(el_{Nat}(x)) =_{El(Nat)} el_{Nat}(m')|$. Therefore $\vDash E(m, m')$. So there exists $k \in E(m, m')$. Hence $m = m'$. Therefore there exists a unique $g : \mathbb{N} \to \mathbb{N}$ such that for all $x \in \mathbb{N}$, $\varphi_e(x) \downarrow\in |f(el_{Nat}(x)) =_{El(Nat)} el_{Nat}(g(x))|$. Hence $e \in \forall x \in Nat, |f(el_{Nat}(x)) =_{El(Nat)} el_{Nat}(g(x))|$. Therefore $\vDash \forall x \in Nat, |f(el_{Nat}(x)) =_{El(Nat)} el_{Nat}(g(x))|$.

Assume $h : \mathbb{N} \to \mathbb{N}$ such that $\vDash \forall x \in Nat, |f(el_{Nat}(x)) =_{El(Nat)} el_{Nat}(h(x))|$. Hence $\vDash \forall x \in \mathbb{N}, E(x, x) \Rightarrow E(g(x), h(x))$. So, there exists $e \in \forall x \in \mathbb{N}, E(x, x) \Rightarrow E(g(x), h(x))$. Therefore, φ_e exists, and for all $x \in \mathbb{N}$, $\varphi_e(x) \downarrow\in E(g(x), h(x))$. Hence $\varphi_e(x) = g(x) = h(x)$. Therefore $g = h$.

If we choose $g = h$, then there exists e such that φ_e exists, and for all $x \in \mathbb{N}$, $\varphi_e(x) \downarrow= g(x)$. Therefore g is computable.

□

This theorem itself motivates the construction of effective topos and it allows us to construct computable functions from our framework.

4 Conclusion

We have built a realisability framework and with a different but equivalent definition of the Effective Topos, we have proved that the Effective Topos was a topos with an object of natural integers simply by using the high-level part of this framework (Theorems 10, 13, 16, 18, 20 and 23) and adapting the proof that the category of sets is a topos. The only difference is that when constructing a morphism, we have to check stability which is always straightforward with the stability properties. Moreover, most of the construction of the high-level of the framework is facilitated by Theorems 6 and 7.

With this framework we can manipulates algebraic types because we have integers and the power of Topos Theory. But it would be better to have the algebraic types as a core feature of the framework.

As a future work we could make a typing system of high order logic where the syntax would be trivially inspired of the high-level part of the framework: the framework would be a trivial model of this system and this would prove the correctness of the system and the ability of extracting proofs. We should use an extended version which manipulates for example dependent types which could be integrated in a future version of this framework.

Therefore, without having any knowledge about category or topos theory, this framework can be a solid ground for future work in an intuitionistic higher-order logic system with interesting properties on the equality.

References

[Fre11] J. Frey. A 2-Categorical Analysis of the Tripos-to-Topos Construction. 2011. 59 pages. Available at http://hal.archives-ouvertes.fr/hal-00698461 2

[Hyl82] J. Hyland. The effective topos. In A. Troelstra and D. V. Dalen, editors, *The L.E.J. Brouwer Centenary Symposium*, pages 165–216. North Holland Publishing Company, 1982. 1, 2, 3

[Law64] B. Lawvere. An elementary theory of the category of sets. *Proceedings of the National Academy of Sciences of the United States of America*, 52:1506–1511, 1964. 1

[Pho92] W.-S. Phoa. An introduction to fibrations, topos theory, the effective topos and modest sets. Technical Report ECS-LFCS-92-208, Department of Computer Science, University of Edinburgh, 1992. 1

[Pit81] A. Pitts. *The Theory of Triposes*. PhD thesis, Cambridge University, 1981. 2

A Full proofs

Lemma 5 (Basic relation between the low level and the high level)
If X is an effective set then:

1. $\vDash \forall u, v \in |El(X)|, |u =_{El(X)} u| \Rightarrow (\forall x \in |X|, u(x) \Leftrightarrow v(x)) \Rightarrow |u =_{El(X)} v|$
2. $\vDash \forall u, v \in El(X), (\forall x \in |X|, u(x) \Rightarrow v(x)) \Rightarrow |u =_{El(X)} v|$
3. $\vDash \forall u \in |El(X)|, |u =_{El(X)} el_X(x)| \Leftrightarrow (|u =_{El(X)} u| \wedge u(x))$
4. $\vDash \forall x, y \in |X|, |x =_X y| \Leftrightarrow |el_X(x) =_{El(X)} el_X(y)|$
5. $\vDash \forall u \in |El(X)|, |u =_{El(X)} u| \Leftrightarrow \exists x \in |X|, |u =_X el_X(x)|$

Proof:

1. $|u =_{El(X)} u|$. Hence, all the properties of $|u =_{El(X)} v|$ that do not talk about v are true (stability, unicity and existence). Therefore, with the equivalence of u and v we have $|u =_{El(X)} v|$.
2. From the previous point, we only have to prove that if $v(x)$ then $u(x)$ for all $x \in |X|$: Assume we have $v(x)$. From $|u =_{El(X)} u|$, there exists y such that $u(y)$. By hypothesis, we have $v(y)$. From $|v =_{El(X)} v|$ we have $|y =_X x|$. Therefore, from $|u =_{El(X)} u|$, we have $u(x)$.
3. - If $|u =_{El(X)} el_X(x)|$ then by symmetry and transitivity we have $|u =_{El(X)} u|$. Also, there exists $y \in |X|$ such that $u(y)$. So we have $el_X(x)(y)$ which means $|x =_X y|$. Therefore, $|y =_X x|$ and $u(x)$ (stability of u).
   - Assume we have $|u =_{El(X)} u|$ and $u(x)$. Let y such that $u(y)$, so we have $|x =_X y|$ (by unicity). Let y such that $|x =_X y|$, so we have $u(y)$ (stability). Hence, for all $y \in |X|$, $u(y)$ if and only if $el_X(x)(y)$. Therefore, from the first point we have $|u =_{El(X)} el_X(x)|$.
4. - Assume $|x =_X y|$.
     - (Stability) If $|x =_X z|$ and $|z =_X z'|$ then $|x =_X z'|$.
     - (Unicity) If $|x =_X z|$ and $|x =_X z'|$ then $|z =_X z'|$.
     - (Existence) $|x =_X y|$ so there exists z such that $|x =_X z|$.
     - (Equivalence) $|x =_X z|$ if and only if $|y =_X z|$.

     Therefore $|el_X(x) =_{El(X)} el_X(y)|$.
   - Assume $|el_X(x) =_{El(X)} el_X(y)|$.

     So there exists z such that $el_X(x)(z)$. Hence $el_X(y)(z)$. Therefore we have $|x =_X z|$ and $|y =_X z|$. Hence $|x =_X y|$.
5. - Assume $|u =_{El(X)} u|$. So there exists x such that $u(x)$. Therefore we have $|u =_{El(X)} el_X(x)|$ from the third point.
   - Assume there exists x such that $|u =_{El(X)} el_X(x)|$. From the third point we have $|u =_{El(X)} u|$.

□

Theorem 7 (Existence and unicity of extensions of functions)
Assume X_1, ... X_n, and Y effective sets, $f : X_1 \to \ldots X_n \to El(Y)$ and $k \leq n$.
We construct $g \in (|El(X_1)| \times ... \times |El(X_k)| \times |X_{k+1}| \times ... \times |X_n|) \to |El(Y)|$ defined by:

$$g(u_1, \ldots, u_k, x_{k+1} \ldots x_n)(y) := \quad \exists x_1 \in |X_1|, ..., x_k \in |X_k|, \; u_1(x_1) \wedge ... \wedge u_k(x_k) \wedge f(x_1, ..., x_n)(y)$$

Then:

- *g is an extension of f on the first k arguments.*
- *For all h extension of f on the first k arguments we have $h \approx g$*

Proof:

- If $|u_1 =_{El(X_1)} u'_1|, \ldots |u_k =_{El(X_k)} u'_k|, |x_{k+1} =_{X_{k+1}} x'_{k+1}|, \ldots |x_n =_{X_n} x'_n|$: we want to prove that $|g(u_1, \ldots u_k, x_{k+1}, \ldots x_n) =_{El(Y)} g(u'_1, \ldots u'_k, x'_{k+1}, \ldots x'_n)|$.
  - If $g(u_1, \ldots u_k, x_{k+1}, \ldots x_n)(y)$ and $|y =_Y y'|$ then there exist $x_1 \in |X_1|, \ldots x_k \in |X_k|$, such that $u_1(x_1), \ldots u_k(x_k)$ and $f(x_1, \ldots x_n)(y)$. Then we have $|x_1 =_{X_1} x_1|, \ldots |x_k =_{X_k} x_k|$. Moreover we have $|x_{k+1} =_{X_{k+1}} x_{k+1}|, \ldots |x_n =_{X_n} x_n|$. Hence $|f(x_1, \ldots x_n) =_{El(Y)} f(x_1, \ldots x_n)|$. So $f(x_1, \ldots x_n)(y')$. Hence we have $g(u_1, \ldots u_k, x_{k+1}, \ldots x_n)(y)$
  - If $g(u_1, \ldots u_k, x_{k+1}, \ldots x_n)(y)$ and $g(u_1, \ldots u_k, x_{k+1}, \ldots x_n)(y')$ then there exist $x_1, x'_1 \in |X_1|, \ldots x_k, x'_k \in |X_k|$ such that $u_1(x_1), \ldots u_k(x_k), u_1(x'_1), \ldots u_k(x'_k), f(x_1, \ldots x_n)(y)$ and $f(x'_1, \ldots x'_k, x_{k+1}, \ldots x_n)(y')$. Therefore we have $|x_1 =_{X_1} x'_1|, \ldots |x_k =_{X_k} x'_k|$. We also have $|x_{k+1} =_{X_{k+1}} x_{k+1}|, \ldots |x_n =_{X_n} x_n|$. Hence $|f(x_1, \ldots x_n) =_{El(Y)} f(x'_1, \ldots x'_k, x_{k+1}, \ldots x_n)|$. So we have $f(x_1, \ldots x_n)(y')$. And then $|y =_Y y'|$.
  - $|u_1 =_{El(X_1)} u_1|, \ldots |u_k =_{El(X_k)} u_k|$, so there exist $x_1 \in |X_1|, \ldots x_k \in |X_k|$, such that $u_1(x_1), \ldots u_k(x_k)$. Then we have $|x_1 =_{X_1} x_1|, \ldots |x_k =_{X_k} x_k|$. Hence $|f(x_1, \ldots x_n) =_{El(Y)} f(x_1, \ldots x_k, x'_{k+1}, \ldots x'_n)|$. So there exists $y \in |Y|$, such that $f(x_1, \ldots x_n)(y)$. Then we have $g(u_1, \ldots, u_k, x_{k+1}, \ldots x_n)(y)$. Hence there exists $y \in |Y|$ such that $g(u_1, \ldots u_n, x_{k+1}, \ldots x_n)(y)$.
  - If $g(u_1, \ldots u_k, x_{k+1}, \ldots x_n)(y)$ then there exist $x_1 \in |X_1|, \ldots x_k \in |X_x|$ such that $u_1(x_1), \ldots u_k(x_k)$ and $f(x_1, \ldots x_n)(y)$. So we have $u'_1(x_1), \ldots u'_k(x_k)$. Moreover, $|x_1 =_{X_1} x_1|, \ldots |x_k =_{X_k} x_k|$. Therefore $|f(x_1, \ldots x_n) =_{El(Y)} f(x_1, \ldots x_k, x'_{k+1}, \ldots x'_n)|$. Hence, $f(x_1, \ldots x_k, x'_{k+1}, \ldots x'_n)(y)$. So we have $g(u'_1, \ldots u'_k, x'_{k+1}, \ldots x'_n)(y)$.
  - With a similar argument, if $g(u'_1, \ldots u'_k, x'_{k+1}, \ldots x'_n)(y)$ then $g(u_1, \ldots u_k, x_{k+1}, \ldots x_n)(y)$.

  Hence $|g(u_1, \ldots u_k, x_{k+1} \ldots x_n) =_{El(Y)} g(u'_1, \ldots u'_k, x'_{k+1}, \ldots x'_n)|$. Therefore $g : El(X_1) \to \ldots El(X_k) \to \ldots X_{k+1} \to \ldots X_n \to El(Y)$.

- If $|x_1 =_{X_1} x_1|, \ldots |x_n =_{X_n} x_n|$:
  - Then $|f(x_1, \ldots x_n) =_{El(Y)} f(x_1, \ldots x_n)|, |el_{X_1}(x_1) =_{El(X_1)} el_{X_1}(x_1)|, \ldots |el_{X_k}(x_k) =_{El(X_k)} el_{X_k}(x_k)|$, and

  $$|g(el_{X_1}(x_1), \ldots el_{X_k}(x_k), x_{k+1}, \ldots x_n) =_{El(Y)} g(el_{X_1}(x_1), \ldots el_{X_k}(x_k), x_{k+1}, \ldots x_n)|$$

  .
  - If $g(el_{X_1}(x_1), \ldots el_{X_k}(x_k), x_{k+1}, \ldots x_n)(y)$ then there exist $x'_1 \in |X_1|, \ldots x'_k \in |X_k|$ such that $el_{X_1}(x_1)(x'_1), \ldots el_{X_k}(x_k)(x'_k)$ and $f(x'_1, \ldots x'_k, x_{k+1}, \ldots x_n)(y)$. Hence $|x_1 =_{X_1} x'_1|, \ldots |x_k =_{X_k} x'_k|$. So we have $|f(x_1, \ldots x_n) =_{El(Y)} f(x'_1, \ldots x'_k, x_{k+1}, \ldots x_n)|$. Hence we have $f(x_1, \ldots x_n)(y)$.

  Hence we have $|g(el_{X_1}(x_1), \ldots el_{X_k}(x_k), x_{k+1}, \ldots x_n) =_{El(Y)} f(x_1, \ldots x_n)|$. Therefore, g is an extension of f on the first k arguments.

- If h is an extension of f on the first k arguments. We construct $F \in (|El(X_1)| \times \ldots |El(X_k)| \times |X_{k+1}| \times \ldots |X_n|) \to Prop$ defined by:

  $$F(u_1, \ldots u_k, x_{k+1}, \ldots x_n) := \ |g(u_1, \ldots u_k, x_{k+1}, \ldots x_n) =_Y h(u_1, \ldots u_k, x_{k+1}, \ldots x_n)|$$

  . By stability of g and h we have $F \in SP(El(X_1), \ldots El(X_k), X_{k+1}, \ldots X_n)$.

  If $|x_1 =_{X_1} x_1|, \ldots |x_n =_{X_n} x_n|$ then we have $|g(el_{X_1}(x_1), \ldots el_{X_k}(x_k), x_{k+1}, \ldots x_n) =_{El(Y)} f(x_1, \ldots x_n)|$ and $|h(el_{X_1}(x_1), \ldots el_{X_k}(x_k), x_{k+1}, \ldots x_n) =_{El(Y)} f(x_1, \ldots x_n)|$. Hence $F(el_{X_1}(x_1), \ldots el_{X_k}(x_k), x_k$

  By Theorem 6, we can prove that:

  $\vDash \forall u_1 \in El(X_1), \ldots u_k \in El(X_k), x_{k+1} \in X_{k+1}, \ldots x_n \in X_n, F(u_1, \ldots u_n, x_{k+1}, \ldots x_n)$

  Therefore $g \approx h$.

□

Lemma 8 (Correctness of composition) *Assume X, Y and Z are effective sets:*

- *If $f : X \to Y$ and $g : Y \to Z$, then $g \circ f : X \to Z$.*
- *If $f : X \to Y$, $f' : X \to Y$, $g : Y \to Z$, $g' : Y \to Z$, $f \approx f'$ and $g \approx g'$, then $g \circ f \approx g' \circ f'$.*

Proof:

- If $|u =_{El(X)} u'|$ then $|f(u) =_{El(Y)} f(u')|$ because $f : X \to Y$. Hence $|g(f(u)) =_{El(Z)} g(f(u'))|$ because $g : Y \to Z$. Therefore $g \circ f : X \to Z$.
- If $|u =_{El(X)} u|$ then $|f(u) =_{El(Y)} f'(u)|$ because $f \approx f'$. So $|f(u) =_{El(Y)} f(u)|$ by symmetry and transitivity. Therefore $|g(f(u)) =_{El(Z)} g'(f(u))|$ because $g \approx g'$. We also have $|g'(f(u)) =_{El(Z)} g'(f'(u))|$ because $g' : Y \to Z$. Hence, by transitivity, we have $|g(f(u)) =_{El(Z)} g'(f'(u))|$. Therefore $g \circ f \approx g' \circ f'$.

□

Theorem 10 (Properties of 1)

- $\models | <>=_1<> |$
- $\models \forall u, v \in El(1), |u =_1 v|$

Proof:

- We have $|() =_1 ()|$ by definition of 1. By Lemma 5.4 we have $|el_1(()) =_{El(1)} el_1(())|$. Therefore $| <>=_{El(1)}<> |$.
- We construct $F \in (|El(1)| \times |El(1)|) \to Prop$ defined by $F(u, v) := \ |u =_{El(1)} v|$. It is trivial that $F \in SP(El(1), El(1))$.

  If $|x =_1 x|$ and $|y =_1 y|$: By definition of 1, we have $|x =_1 y|$. Then by Lemma 5.4 we have $|el_1(x) =_{El(1)} el_1(y)|$. Therefore $F(el_1(x), el_1(y))$.

  By Theorem 6 we have $\models \forall u, v \in El(1), F(u, v)$. Then we can conclude.

□

Theorem 11 (C has a final object) *1 is the final object of* ***C****.*

Proof:

Assume X is an effective set.
We construct $f \in |El(X)| \to |El(1)|$ defined by: $f(u) := <>$.

- Stability of f: If $|u =_{El(X)} u'|$ then by Theorem 10 we have $| <>=_{El(1)}<> |$. Hence $|f(u) =_{El(1)} f(u')|$. Therefore $f : El(X) \to El(1)$.
- Unicity of f: Assume $g : El(X) \to El(1)$. If $|u =_{El(X)} u|$, then, because $f, g : El(X) \to El(1)$, we have $|f(u) =_{El(1)} f(u)|$ and $|g(u) =_{El(1)} g(u)|$. By Theorem 10 we have $|f(u) =_{El(1)} g(u)|$. Therefore $f \approx g$.

Hence, 1 is a final object of **C**.

□

Lemma 12 (Stability of p'_1, p'_2 and $cons'$)
$p'_1 : (A \times B) \to El(A)$, $p'_2 : (A \times B) \to El(B)$ *and* $cons' : A \to B \to El(A \times B)$.

Proof:

- If $|c =_{A\times B} c'|$ then by definition of $A \times B$ we have $|\pi_1(c) =_A \pi_1(c')|$. So $|el_A(\pi_1(c)) =_{El(A)} el_A(\pi_1(c'))|$. Hence $|p'_1(c) =_{El(A)} p'_1(c')|$. Therefore $p'_1 : (A \times B) \to El(A)$.
- With the same kind of proof, we have $p'_2 : (A \times B) \to El(B)$.
- If $|a =_A a'|$ and $|b =_B b'|$ then $|\pi_1(a, b) =_A \pi_1(a', b')|$ and $|\pi_2(a, b) =_B \pi_2(a', b')|$. By definition of $A \times B$ we have $|(a, b) =_{A\times B} (a', b')|$. So, $|el_{A\times B}(a, b) =_{El(A\times B)} el_{A\times B}(a', b')|$. Hence $|cons'(a, b) =_{El(A\times B)} cons'(a', b')|$. Therefore $cons' : A \to B \to El(A \times B)$.

□

Theorem 13 (Properties of $A \times B$)

Assume A and B are effective sets.

- $\models \forall w, w' \in |El(A \times B)|, |w =_{El(A\times B)} w'| \Rightarrow |p_1(w) =_{El(A)} p_1(w')|$
- $\models \forall w, w' \in |El(A \times B)|, |w =_{El(A\times B)} w'| \Rightarrow |p_2(w) =_{El(B)} p_2(w')|$
- $\models \forall u, u' \in |El(A)|, v, v' \in |El(B)|,$
  $|u =_{El(A)} u'| \Rightarrow |v =_{El(B)} v'| \Rightarrow |< u, v >=_{El(A\times B)}< u', v' > |$
- $\models \forall u \in El(A), v \in El(B), |p_1(< u, v >) =_{El(A)} u|$
- $\models \forall u \in El(A), v \in El(B), |p_2(< u, v >) =_{El(B)} v|$
- $\models \forall w, w' \in El(A \times B), |p_1(w) =_{El(A)} p_1(w')| \Rightarrow |p_2(w) =_{El(B)} p_2(w')| \Rightarrow |w =_{El(A\times B)} w'|$

Proof:

- The first three properties are just expressing the stability of p_1, p_2 and *cons* which theu are by construction.
- We use Theorem 6: We construct $F \in (|El(A)| \times |El(B)|) \rightarrow Prop$ defined by: $F(u, v) := |p_1(cons(u, v)) =_{El(A)} u|$. By stability of p_1 and *cons* we have $F \in SP(El(A), El(B))$.

  If $|a =_A a|$ and $|b =_B b|$ then by definition of *cons* we have $|cons(el_A(a), el_B(b)) =_{El(A\times B)} el_{A\times B}((a, b))|$. Hence, $|p_1(cons(el_A(a), el_B(b))) =_{El(A)} p_1(el_{A\times B}((a, b)))|$. Moreover, we have $|(a, b) =_{A\times B} (a, b)|$ (because $|\pi_1(a, b) =_A \pi_1(a, b)|$ and $|\pi_2(a, b) =_B \pi_2(a, b)|$). By definition of p_1 we have $|p_1(el_{A\times B}(a, b)) =_{El(A\times B)} el_A(\pi_1(a, b))|$ with $\pi_1(a, b) = a$. Hence, by transitivity, we have $|p_1(cons(el_A(a), el_B(b))) =_{El(A)} el_A(a)|$. Therefore, $F(el_A(a), el_B(b))$. By Theorem 6 we have $\models \forall u \in El(A), v \in El(B), F(u, v)$. Then we can conclude.
- With the same kind of proof as above we can prove the other β-reduction (with p_2).
- We use Theorem 6: We construct $F \in (|El(A \times B)| \times |El(A \times B)|) \rightarrow Prop$ defined by:

  $$F(w, w') := |p_1(w) =_{El(A)} p_1(w')| \Rightarrow |p_2(w) =_{El(B)} p_2(w')| \Rightarrow |w =_{El(A\times B)} w'|$$

  By stability of p_1 and p_2, we have $F \in SP(El(A \times B), El(A \times B))$.

  If $|c =_{A\times B} c|$, $|c' =_{A\times B} c'|$, $|p_1(el_{A\times B}(c)) =_{El(A)} p_1(el_{A\times B}(c'))|$ and $|p_2(el_{A\times B}(c)) =_{El(B)} p_2(el_{A\times B}(c'))|$: Then by definition of p_1, $|p_1(el_{A\times B}(c)) =_{El(A)} el_A(\pi_1(c))|$ and $|p_1(el_{A\times B}(c')) =_{El(A)} el_A(\pi_1(c'))|$. By symmetry and transitivity, $|el_A(\pi_1(c)) =_{El(A)} el_A(\pi_1(c'))|$. Hence $|\pi_1(c) =_A \pi_1(c')|$. We can also prove that $|\pi_2(c) =_B \pi_2(c')|$. By definition of $A \times B$, $|c =_{A\times B} c'|$. And then $|el_{A\times B}(c) =_{El(A\times B)} el_{A\times B}(c')|$.

  By Theorem 6 we have $\models \forall w, w' \in El(A \times B), F(w, w')$. Then we can conclude.

□

Theorem 14 (C has products)

If A and B effective sets, then $A \times B$ is the product of A and B in $\boldsymbol{C}$, p_1 and p_2, its projections. Hence $\boldsymbol{C}$ is cartesian.

Proof:

$A \times B$ is an effective set, $p_1 : El(A \times B) \rightarrow El(A)$ and $p_2 : El(A \times B) \rightarrow El(B)$.
Assume X is an effective set, $f : El(X) \rightarrow El(A)$ and $g : El(X) \rightarrow El(B)$.
We construct $\varphi \in |El(X)| \rightarrow |El(A \times B)|$ defined by: $\varphi(u) := < f(u), g(u) >$.

- Stability of φ: If $|u =_{El(X)} u'|$ then $|f(u) =_A f(u')|$ by stability of f. By stability of g we also have $|g(u) =_B g(u')|$. So, by stability of *cons*, $| < f(u), g(u) >=_{A\times B}< f(u'), g(u') > |$. Hence, $|\varphi(u) =_{A\times B} \varphi(u')|$. Therefore $\varphi : El(X) \rightarrow El(A \times B)$.
- If $|u =_{El(X)} u|$ then $|f(u) =_{El(A)} f(u)|$ and $|g(u) =_{El(B)} g(u)|$. By Theorem 13 we have $|p_1(< f(u), g(u) >) =_{El(A)} f(u)|$. Hence $|(p_1 \circ \varphi)(u) =_{El(A)} f(u)|$. Therefore, $p_1 \circ \varphi \approx f$.
- By a similar argument we can also prove that $p_2 \circ \varphi \approx g$.

- Assume $\psi : El(X) \to El(A \times B)$ such that $p_1 \circ \psi \approx f$ and $p_2 \circ \psi \approx g$.

  If $|u =_{El(X)} u|$ then $|\varphi(u) =_{El(A\times B)} \varphi(u)|$, $|\psi(u) =_{El(A\times B)} \psi(u)|$, $|p_1(\varphi(u)) =_{El(A)} f(u)|$ and $|p_1(\psi(u)) =_{El(A)} f(u)|$. So, $|p_1(\varphi(u)) =_{El(A)} p_1(\psi(u))|$. We can also prove that $|p_2(\varphi(u)) =_{El(B)} p_2(\psi(u))|$. Hence, by Theorem 13, $|\varphi(u) =_{El(A\times B)} \psi(u)|$. Therefore $\varphi \approx \psi$.

□

Lemma 15 (Stability of app'**)** $app' : (A \Rrightarrow B) \to El(A) \to El(B)$

Proof:
If $|f =_{A\Rrightarrow B} f'|$ and $|u =_{El(A)} u'|$ then by definition of $A \Rrightarrow B$ we have $|f(u) =_{El(B)} f'(u)|$. Hence $|app'(f, u) =_{El(B)} app'(f', u')|$. Therefore $app' : (A \Rrightarrow B) \to El(A) \to El(B)$.

□

Theorem 16 (Properties of $A \Rrightarrow B$**)** *Assume A and B are effective sets.*

- $\models \forall w, w' \in |El(A \Rrightarrow B)|, u, u' \in |El(A)|,$
  $|w =_{El(A)} w'| \Rightarrow |u =_{El(A)} u'| \Rightarrow |app(w, u) =_{El(B)} app(w', u')|$
- $\models \forall f, f' \in |El(A)| \to |El(B)|, (\forall u, u' \in |El(A)|,$
  $|u =_{El(A)} u'| \Rightarrow |f(u) =_{El(B)} f'(u')|) \Rightarrow |\Lambda u : A.f(u) =_{El(A\Rrightarrow B)} \Lambda u : A.f'(u)|$
- $\models \forall f \in |El(A)| \to |El(B)|, u \in El(A),$
  $(\forall v, v' \in |El(A)|, |v =_{El(A)} v'| \Rightarrow |f(v) =_{El(B)} f(v')|)$
  $\Rightarrow |app((\Lambda v : A.f(v)), u) =_{El(B)} f(u)|$
- $\models \forall w, w' \in El(A \Rrightarrow B), (\forall u \in El(A), |app(w, u) =_{El(B)} app(w', u)|) \Rightarrow |w =_{El(A\Rrightarrow B)} w'|$

Proof:

- The first point is just expressing the stability of *app*.
- The second point is just an way of expressing that if $|f =_{A\Rrightarrow B} f'|$ then $|el_{A\Rrightarrow B}(f) =_{El(A\Rrightarrow B)} el_{A\Rrightarrow B}(f')|$.
- The third point is just another way of expressing that *app* is an extension of app' on the first argument.
- We use Theorem 6: We construct $F \in (|El(A \Rrightarrow B)| \times |El(A \Rrightarrow B)|) \to Prop$ defined by:

  $$F(w, w') := (\forall u \in El(A), |app(w, u) =_{El(B)} app(w', u)|) \Rightarrow |w =_{El(A\Rrightarrow B)} w'|$$

  By stability of *app*, $F \in SP(El(A \Rrightarrow B), El(A \Rrightarrow B))$.

  If $|f =_{A\Rrightarrow B} f|$, $|f' =_{A\Rrightarrow B} f'|$ and $\forall u \in El(A), |app(el_{A\Rrightarrow B}(f), u) =_{El(B)} app(el_{A\Rrightarrow B}(f'), u)|$: Let $u, u' \in |El(A)|$ such that $|u =_{El(A)} u'|$. So $|u =_{El(A)} u|$. By definition of *app*, $|app(el_{A\Rrightarrow B}(f), u) =_{El(B)} f(u)|$. By hypothesis, $|app(el_{A\Rrightarrow B}(f), u) =_{El(B)} app(el_{A\Rightarrow B}(f'), u)|$. We can also prove that $|app(el_{A\Rrightarrow B}(f'), u') =_{El(B)} f'(u')|$. Hence $|f(u) =_{El(B)} f(u')|$. Therefore $|f =_{A\Rrightarrow B} f'|$ and $|el_{A\Rrightarrow B}(f) =_{El(A\Rrightarrow B)} el_{A\Rrightarrow B}(f')|$.

  By Theorem 6 we have $\models \forall w, w' \in El(A \Rrightarrow B), F(w, w')$. Then we can conclude.

□

Theorem 17 (C has power objects) *If A and B effective sets then $A \Rrightarrow B$ with $ev : El((A \Rrightarrow B) \times A) \to El(B)$ defined by $ev(w) := app(p_1(w), p_2(w))$ is B power A in **C**.*
*Hence **C** is cartesian and closed.*

Proof:
$A \Rrightarrow B$ is an effective set.
By stability of *app*, p_1 and p_2 we have $ev : El((A \Rrightarrow B) \times A) \to El(B)$
Assume X is an effective set and $f : El(X \times A) \to El(B)$.
We construct $\varphi \in |El(X)| \to |El(A \Rrightarrow B)|$ defined by $\varphi(u) := \Lambda v : A.f(< u, v >)$.

- If $|u =_{El(X)} u'|$: If $|v =_{El(A)} v'|$ then $| < u, v >=_{El(X\times A)} < u', v' > |$. So $|f(< u, v >) =_{El(B)} f(< u', v' >)|$. By Theorem 16 we have $|\varphi(u) =_{El(A\Rrightarrow B)} \varphi(u')|$. Therefore $\varphi : El(X) \to El(A \Rrightarrow B)$.
- If $|w =_{El(X\times A)} w|$: Then $|p_1(w) =_{El(X)} p_1(w)|$ and $|p_2(w) =_{El(A)} p_2(w)|$. For all v, v' in $|El(A)|$, if $|v =_{El(A)} v'|$ then $|f(< p_1(w), v >) =_{El(B)} f(< p_1(w), v' >)|$. By theorem 16 we have $|app((\Lambda v : A.f(< p_1(w), v >)), p_2(w)) =_{El(B)} f(< p_1(w), p_2(w) >)|$. Hence $|app(\varphi(p_1(w)), p_2(w)) =_{El(B)} f(< p_1(w), p_2(w) >)|$. Moreover:

$$| < p_1(w), p_2(w) >=_{El(X\times A)} < p_1(w), p_2(w) > |$$
$$|p_1(< p_1(w), p_2(w) >) =_{El(X)} p_1(w)|$$
$$|p_2(< p_1(w), p_2(w) >=_{El(A)} p_2(w)|$$

  So $| < p_1(w), p_2(w) >=_{El(X\times A)} w|$. Then, $|f(< p_1(w), p_2(w) >) =_{El(B)} f(w)|$. Hence $|app(\varphi(p_1(w)), p_2(w)) =_{El(B)} f(w)|$. Therefore
  $\vDash \forall w \in El(X \times A), |app(\varphi(p_1(w)), p_2(w)) =_{El(B)} f(w)|$.
- Assume $\psi : El(X) \to El(A \Rrightarrow B)$ such that $\vDash \forall w \in El(X \times A), |app(\psi(p_1(w)), p_2(w)) =_{El(B)} f(w)|$.

  If $|u =_{El(X)} u|$:
  - Then we have $|\varphi(u) =_{El(A\Rrightarrow B)} \varphi(u)|$ and $|\psi(u) =_{El(A\Rrightarrow B)} \psi(u)|$.
  - If $|v =_{El(A)} v|$: Then $| < u, v >=_{El(X\times A)} < u, v > |$. Therefore $|app(\varphi(p_1(< u, v >)), p_2(< u, v >)) =_{El(B)} f(< u, v >)|$ and $|app(\psi(p_1(< u, v >)), p_2(< u, v >)) =_{El(B)} f(< u, v >)|$. We also have $|p_1(< u, v >) =_{El(X)} u|$ and $|p_2(< u, v >) =_{El(A)} v|$. So, $|\varphi(p_1(< u, v >)) =_{El(A\Rrightarrow B)} \varphi(u)|$. Hence, $|app(\varphi(p_1(< u, v >), p_2(< u, v >) =_{El(B)} app(\varphi(u), v)|$. We can also prove that $|app(\psi(p_1(< u, v >), p_2(< u, v >)) =_{El(B)} app(\psi(u), v|$. Hence, $|app(\varphi(u), v) =_{El(B)} app(\psi(u), v)|$.

  By Theorem 16, we have $|\varphi(u) =_{El(A\Rrightarrow B)} \psi(u)|$. Therefore $\varphi \approx \psi$.

Then we can conclude.

□

Theorem 18 (Properties of Ω)

- $\vDash \forall q, q' \in Prop, (q \Leftrightarrow q') \Leftrightarrow |el_\Omega(q) =_{El(\Omega)} el_\Omega(q')|$
- $\vDash \forall u, v \in |El(\Omega)|, |u =_{El(\Omega)} v| \Rightarrow (prop(u) \Leftrightarrow prop(v))$
- $\vDash \forall q \in Prop, prop(el_\Omega(q)) \Leftrightarrow q$
- $\vDash \forall u, v \in El(\Omega), (prop(u) \Leftrightarrow prop(v)) \Rightarrow |u =_{El(\Omega)} v|$

Proof:

- $q \Leftrightarrow q'$ if and only if $|q =_\Omega q'|$, if and only if $|el_\Omega(q) =_{El(\Omega)} el_\Omega(q')|$.
- Assume $|u =_{El(\Omega)} v|$: $prop(u)$ if and only if $u(\top)$ if and only if $v(\top)$, if and only if $prop(v)$.
- $prop(el_\Omega(q))$ if and only if $el_\Omega(q)(\top)$, if and only if $q \Leftrightarrow \top$, if and only if q.
- We construct $F \in (|El(\Omega)| \times |El(\Omega)|) \to Prop$ defined by: $F(u, v) := (prop(u) \Leftrightarrow prop(v)) \Rightarrow |u =_{El(\Omega)} v|$. By stability of $prop$, $F \in SP(El(\Omega), El(\Omega))$.

  If $prop(el_\Omega(q)) \Leftrightarrow prop(el_\Omega(q'))$, then $q \Leftrightarrow q'$. So $|el_\Omega(q) =_{El(\Omega)} el_\Omega(q')|$.

  By Theorem 6, we have $\vDash \forall u, v \in El(\Omega), F(u, v)$. Then we can conclude.

□

Theorem 19 (Properties of $True$) *We have $True : El(1) \to El(\Omega)$.*
Furthermore, assume that X is an effective set.
Then for all $f : El(X) \to El(\Omega)$, $f \approx True \circ *$ if and only if $\models \forall u \in El(X), prop(f(u))$

Proof:

- Stability of $True$: We have $\top \Leftrightarrow \top$. Then $|el_\Omega(\top) =_{El(\Omega)} el_\Omega(\top)|$. Hence, $|True(u) =_{El(\Omega)} True(u')|$. Therefore $True : El(1) \to El(\Omega)$
- Remark: For all $u \in |El(X)|$, $(True \circ *)(u) = el_\Omega(\top)$.
- If $|u =_{El(X)} u|$ and $|f(u) =_{El(\Omega)} el_\Omega(\top)|$ then $prop(f(u)) \Leftrightarrow prop(el_\Omega(\top))$. We also have $prop(el_\Omega(\top)) \Leftrightarrow \top$. Therefore, we have $prop(f(u))$.
- If $|u =_{El(X)} u|$ and $prop(f(u))$ then $|f(u) =_{El(\Omega)} f(u)|$ and $|(True \circ *)(u) =_{El(\Omega)} (True \circ *)(u)|$. We also have $prop(f(u)) \Leftrightarrow \top$ and $prop(el_\Omega)(\top) \Leftrightarrow \top$. Hence $prop(f(u)) \Leftrightarrow prop((True \circ *)(u))$. By Theorem 18 we have $|f(u) =_{El(\Omega)} (True \circ *)(u)|$.

Then we can conclude.

□

Theorem 20 (Properties of $\{u \in A \mid F(u)\}$)
Assume A is an effective set and $F \in SP(El(A))$. Let $B := \{u \in A | F(u)\}$. Then:
$\models \forall u, v \in |El(A)|, |u =_{El(B)} v| \Leftrightarrow (|u =_{El(A)} v| \wedge F(u))$

Proof:

- Assume $|u =_{El(B)} v|$:
  - Stability: If $u(a)$ and $|a =_A a'|$ then $|a =_B a|$ since $|u =_{El(B)} v|$. So we have $F(el_A(a))$. Hence $|a =_B a'|$. Therefore $u(a')$.
  - Unicity: If $u(a)$ and $u(a')$, then $|a =_B a'|$ by uncicity for u in B. Hence $|a =_A a'|$.
  - Existence and equivalence still hold (they are independent from the equality).

  Therefore $|u =_{El(A)} v|$. So we have $|u =_{El(A)} u|$. Then there exists $a \in |A|$ such that $|u =_{El(A)} el_A(a)|$. Hence $u(a)$ and $|el_A(a) =_{El(A)} u|$. So, $|a =_B a|$. Hence $F(el_A(a))$. Therefore $F(u)$.
- Assume $|u =_{El(A)} v|$ and $F(u)$:
  - Stability: If $u(a)$ and $|a =_B a'|$ then $|a =_A a'|$. Hence $u(a')$.
  - Unicity: If $u(a)$ and $u(a')$ then $|a =_A a'|$ by unicity in A. We also have $|u =_{El(A)} u|$. Then $|u =_{El(A)} el_A(a)|$ by Lemma 5.3. Hence $F(el_A(a))$. Therefore $|a =_B a'|$.
  - The existence and equivalence still hold.

  Therefore $|u =_{El(B)} v|$.

□

Theorem 21 (C has pullbacks of $True$) *Assume A is an effective set and $f : El(A) \to El(\Omega)$. Then B defined by $B := \{u \in A \mid prop(f(u))\}$ is an effective set and if $i(u) := u$ then $i : El(B) \to El(A)$ and B with i is the pullback of $True$ along f.*

Proof:
By stability of f and $prop$, B is well defined.
If $|u =_{El(B)} u'|$, then by Theorem 20 we have $|u =_{El(A)} u'|$. Hence $|i(u) =_{El(A)} i(u')|$. Therefore $i : El(B) \to El(A)$.
If $|u =_{El(B)} u|$ then by Theorem 20 we have $prop(f(u))$. So, $prop(f(i(u)))$. Hence $\models \forall u \in El(B), prop(f(i(u)))$. Therefore, by Theorem 19, $f \circ i \approx True \circ *$.
Assume X is an effective set and $\varphi : El(X) \to El(A)$ such that $f \circ \varphi \approx True \circ *$. Then $\models \forall u \in El(X), prop(f(\varphi(u)))$. We also have $\varphi \in |El(X)| \to |El(B)|$.
We choose $\psi := \phi$.

- We prove $\psi : El(X) \to El(B)$: If $|u =_{El(X)} u'|$ then $|\varphi(u) =_{El(A)} \varphi(u')|$. We also have $|u =_{El(X)} u|$, so by hypothesis we have $prop(f(\varphi(u)))$. Hence $|\varphi(u) =_{El(B)} \varphi(u')|$. Therefore $\psi : El(X) \to El(B)$.
- If $|u =_{El(X)} u|$ then $|\varphi(u) =_{El(A)} \varphi(u)|$. Hence $|i(\varphi(u)) =_{El(A)} \varphi(u)|$. Therefore $i \circ \varphi \approx \varphi$.
- Assume $\psi' : El(X) \to El(B)$ such that $i \circ \psi' \approx \varphi$. If $|u =_{El(X)} u|$, then $|i(\psi'(u)) =_{El(A)} \varphi(u)|$. So $|\psi'(u) =_{El(A)} \varphi(u)|$. We also have $|\psi'(u) =_{El(B)} \psi'(u)|$. So $prop(f(\psi'(u)))$. Hence $|\psi'(u) =_{El(B)} \varphi(u)|$. Therefore $\psi' \approx \varphi$.

Then we can conclude by choosing φ as ψ.

□

Theorem 22 (Equivalence between monorphisms and injective functions)
Assume A and B effective sets and $m : El(A) \to El(B)$.
m is a monomorphism in $\boldsymbol{C}$ if and only if m is injective.

Proof:

- Assume m is injective. Let X an effective set and $f, g : El(X) \to El(A)$ such that $m \circ f \approx m \circ g$. If $|u =_{El(X)} u|$, then $|f(u) =_{El(A)} f(u)|$, $|g(u) =_{El(A)} g(u)|$ and $|m(f(u)) =_{El(B)} m(g(u))|$. By injectivity, $|f(u) =_{El(A)} g(u)|$. Therefore $f \approx g$.
- Assume m is a monomorphism. We construct the effective set X defined by: $X := \{w \in A \times A \mid |m(p_1(w)) =_{El(B)} m(p_2(w))|$. By stability of m, p_1 and p_2, X is well defined.

  We also construct $f, g \in |El(X)| \to |El(A)|$ defined by: $f := p_1$ and $g := p_2$.
  - If $|w =_{El(X)} w'|$, then $|w =_{El(A\times A)} w'|$ by Theorem 20. So we have $|p_1(w) =_{El(A)} p_1(w')|$. Hence $|f(w) =_{El(A)} f(w')|$. Therefore $f : El(X) \to El(A)$.
  - With the same kind of proof we also have $g : El(X) \to El(A)$.
  - If $|w =_{El(X)} w|$, then $|m(p_1(w)) =_{El(B)} m(p_2(w))|$ by Theorem 20. Hence $|m(f(w)) =_{El(B)} m(g(w))|$. Therefore, $m \circ f \approx m \circ g$.

  By definition of monomorphism, $f \approx g$ (We have defined $f, g : X \to A$ so that we do not confuse them with $p_1, p_2 : El(A \times A) \to El(A)$.).

  If $|u =_{El(A)} u|$, $|v =_{El(A)} v|$ and $|m(u) =_{El(B)} m(v)|$: Then $| < u, v >=_{El(A\times A)} < u, v > |$ and $|p_1(< u, v >) =_{El(A)} u|$. So, $|m(p_1(< u, v >)) =_{El(B)} m(u)|$. We can also prove that $|m(p_2(< u, v >)) =_{El(B)} m(v)|$. Therefore $|m(p_1(< u, v >) =_{El(B)} m(p_2(< u, v >))|$. By Theorem 20 we have $| < u, v >=_{El(X)} < u, v > |$. Hence, $|f(< u, v >) =_{El(A)} g(< u, v >)|$ since $f \approx g$. So, $|p_1(< u, v >) =_{El(A)} p_2(< u, v >)|$. Hence, $|u =_A v|$.

  Therefore m is injective.

□

Theorem 24 (Monomorphisms of C have a caracteristic morphism)
Assume A and B is effective sets, and $m : El(A) \to El(B)$ a monomorphism.
Then we have $\chi_m : El(B) \to El(\Omega)$.
And it is the only morphism (modulo $\approx$) from B to Ω in $\boldsymbol{C}$ such that m is the pullback of $True$ along χ_m.

Proof:

By Theorem 22, m is injective. We also have: $prop(\chi_m(v))$ if and only if there exists $u \in |El(A)|$ such that $|u =_{El(A)} u|$ and $|m(u) =_{El(B)} v|$ by Theorem 18.3.

Stability: If $|v =_{El(B)} v'|$ then: If there exists $u \in El(A)$ such that $|u =_{El(A)} u|$ and $|m(u) =_{El(B)} v|$, then $|m(u) =_{El(B)} v'|$. Hence there exists $u \in |El(A)|$, such that $|u =_{El(A)} u|$ and $|m(u) =_{El(B)} v'|$. We can also prove that if $\exists u \in El(A), |m(u) =_{El(B)} v'|$ then $\exists u \in El(A), |m(u) =_{El(B)} v|$. Therefore $\exists u \in El(A), |m(u) =_{El(B)} v| \Leftrightarrow \exists u \in El(A), |m(u) =_{El(B)} v'|$. Hence $|\chi_m(v) =_{El(\Omega)} \chi_m(v')|$. Therefore $\chi_m : El(B) \to El(\Omega)$.

m pullback: If $|u =_{El(A)} u|$ then $|m(u) =_{El(B)} m(u)|$. So, there exists $u' \in |El(A)|$, such that $|u' =_{El(A)} u'|$ and $|m(u') =_{El(B)} m(u)|$. Hence $prop(\chi_m(m(u)))$. Therefore $\chi_m \circ m \approx True \circ *$ by Theorem 19.

Assume X is an effective set and $\varphi : El(X) \to El(A)$ such that $\chi_m \circ \varphi \approx True \circ *$. Then $\vDash \forall u \in El(A), prop(\chi_m(\varphi(u)))$. For every $w \in |El(X)|$ we construct $F_w \in |El(A)| \to Prop$ defined by: $F_w(u) := |u =_{El(A)} u| \wedge |m(u) =_{El(B)} \varphi(w)|$. We construct $\psi \in |El(X)| \to |El(A)|$ defined by $\psi(w) := d(F_w)$.

- Stability of ψ: If $|w =_{El(X)} w'|$:

  Then $|w =_{El(X)} w|$. So $prop(\chi_m(\varphi(w)))$. Hence, there exists $u \in |El(A)|$ such that $|u =_{El(A)} u|$ and $|m(u) =_{El(B)} \varphi(w)|$. Therefore, there exists $u \in |El(A)|$ such that $F_w(u)$.

  If $F_w(u)$ and $|u =_{El(A)} u'|$ then $|u' =_{El(A)} u'|$, $|m(u) =_{El(B)} \varphi(w)|$ and $|m(u) =_{El(B)} m(u')|$. Hence, $|m(u') =_{El(B)} \varphi(v)|$. Therefore, $F_w(u')$.

  If $F_w(u)$ and $F_w(u')$ then $|m(u) =_{El(B)} \varphi(v)|$ and $|m(u') =_{El(B)} \varphi(v)|$. So, $|m(u) =_{El(B)} m(u')|$. We also have $|u =_{El(A)} u|$ and $|u' =_{El(A)} u'|$. By injectivity, $|u =_{El(A)} u'|$.

  Therefore, by Theorem 23, we have $F_w(d(F_w))$. So, $F_w(\psi(w))$.

  We can also prove that $F_{w'}(\psi(w'))$. So, $|\psi(w') =_{El(A)} \psi(w')|$ and $|m(\psi(w')) =_{El(B)} \varphi(w')|$. We also have $|\varphi(w) =_{El(B)} \varphi(w')|$. Hence, $|m(\psi(w')) =_{El(B)} \varphi(w)|$. Therefore, $F_w(\psi(w'))$.

  By unicity of F_w we have $|\psi(w) =_{El(A)} \psi(w')|$. Therefore $\psi : El(X) \to El(A)$.

- Commutation: If $|w =_{El(X)} w|$ then we can prove that $F_w(\psi(w))$. Hence, $|m(\psi(w)) =_{El(B)} \varphi(w)|$. Therefore $m \circ \psi \approx \varphi$.

- Unicity: Assume $\psi' : El(X) \to El(A)$ such that $m \circ \psi' \approx \varphi$. If $|w =_{El(X)} w|$ then we can prove that $F_w(\psi(w))$ and the unicity of F_w. We also have $|m(\psi'(w)) =_{El(B)} \varphi(w)|$. So, $F_w(\psi'(w))$. By unicity of F_w we have $|\psi(w) =_{El(A)} \psi'(w)|$. Therefore $\psi \approx \psi'$.

Therefore m is the pullback of $True$ along χ_m.

Assume $f : El(B) \to El(\Omega)$ such that m is the pullback of $True$ along f. Theorem 21 gives us $C := \{v \in B \mid prop(f(v))\}$ an effective set and $i : El(C) \to El(B)$. $f \circ i \approx True \circ *$ so there exists $\varphi : El(C) \to El(A)$ such that $m \circ \varphi \approx i$.

If $|v =_{El(B)} v|$ then $|\chi_m(v) =_{El(\Omega)} \chi_m(v)|$, $|f(v) =_{El(\Omega)} f(v|$ and:

- If $prop(\chi_m(v))$ then there exists $u \in |El(A)|$, such that $|u =_{El(A)} u|$ and $|m(u) =_{El(B)} v|$. Therefore, $|f(m(u)) =_{El(\Omega)} f(v)|$. Since $f \circ m \approx True \circ *$ we also have $prop(f(m(u)))$. Hence, $prop(f(v))$.
- If $prop(f(v))$ then $|v =_{El(C)} v|$ by Theorem 20. So, $|\varphi(v) =_{El(A)} \varphi(v)|$ and $|m(\varphi(v)) =_{El(B)} i(v)|$. Hence there exists $u \in |El(A)|$, such that $|u =_{El(A)} u|$ and $|m(u) =_{El(B)} v|$. Therefore $prop(\chi_m(v))$.

By Theorem 18.4 we have $|\chi_m(v) =_{El(\Omega)} f(v)|$. Therefore $\chi_m \approx f$.

□

Lemma 26 (Properties of E)

1. $\vDash E(0, 0)$
2. $\vDash \forall x, y \in \mathbb{N}, E(x, y) \Rightarrow E(s(x), s(y))$
3. $\vDash \forall x, y \in \mathbb{N}, E(x, y) \Rightarrow E(y, x)$
4. $\vDash \forall x, y, z \in \mathbb{N}, E(x, y) \Rightarrow E(y, z) \Rightarrow E(x, z)$
5. $\vDash \forall x, y \in \mathbb{N}, E(s(x), s(y)) \Rightarrow E(x, y)$
6. $\vDash \forall x \in \mathbb{N}, E(s(x), 0) \Rightarrow \bot$
7. *For all* $\vDash \forall P \in \mathbb{N} \to Prop, P(0) \Rightarrow (\forall x \in \mathbb{N}, P(x) \Rightarrow P(s(x))) \Rightarrow$ $\forall x \in \mathbb{N}, E(x, x) \Rightarrow P(x)$

Proof:

- The proof of 1 is just the constant 0.
- The proof of 2 is the successor function.
- The proof of 3 and 6 is the identity function.
- The proof of 4 is just a projection.
- The proof of 5 is the predecessor function.
- The proof of 7 is a function defined by a simple recursion.

□

Theorem 27 (Properties of Nat)

- $\models |Z =_{El(Nat)} Z|$
- $\models \forall u, v \in |El(Nat)|, |u =_{El(Nat)} v| \Rightarrow |S(u) =_{El(Nat)} S(v)|$
- $\models \forall u, v \in El(Nat), |S(u) =_{El(Nat)} S(v)| \Rightarrow |u =_{El(Nat)} v|$
- $\models \forall u \in El(Nat), |S(u) =_{El(Nat)} Z| \Rightarrow \bot$
- *For all* $P \in SP(El(Nat))$,
  if $\models P(Z)$ *and* $\models \forall u \in El(Nat), P(u) \Rightarrow P(S(u))$ *then* $\models \forall u \in El(Nat), P(u)$

Proof:

- $E(0,0)$, so $|0 =_{Nat} 0|$. Hence $|el_{Nat}(0) =_{El(Nat)} el_{Nat}(0)|$. Therefore $|Z =_{El(Nat)} Z|$.
- By stability of S.
- We construct $F \in (|El(Nat)| \times |El(Nat)|) \to Prop$ defined by: $F(u,v) := |S(u) =_{El(Nat)} S(v)| \Rightarrow |u =_{El(Nat)} v|$. By stability of S, we have $F \in SP(El(Nat), El(Nat))$.

  If $|x =_{Nat} x|$, $|y =_{Nat} y|$ and $|S(el_{Nat}(x)) =_{El(Nat)} S(el_{Nat})(y)|$: By definition of S, $|S(el_{Nat}(x)) =_{El(Nat)} el_{Nat}(s(x))|$ and $|S(el_{Nat}(y)) =_{El(Nat)} el_{Nat}(s(y))|$. Hence $|el_{Nat}(s(x)) =_{El(Nat)} el_{Nat}(s(y))|$. Therefore, $E(s(x), s(y))$. By Lemma 26.5, $E(x,y)$. Hence $|el_{Nat}(x) =_{El(Nat)} el_{Nat}(y)|$.

  By Theorem 6 we have $\models \forall u, v \in El(Nat), F(u,v)$. Then we can conclude.
- We construct $F \in |El(Nat)| \to Prop$ defined by: $F(u) := |S(u) =_{El(Nat)} Z| \Rightarrow \bot$. By stability of S we have $F \in SP(El(Nat))$.

  If $|x =_{Nat} x|$ and $|S(el_{Nat}(x)) =_{El(Nat)} Z|$: By definition of S, $|S(el_{Nat}(x)) =_{El(Nat)} el_{Nat}(s(x))|$. Hence $|el_{Nat}(s(x)) =_{El(Nat)} el_{Nat}(0)|$. Therefore $E(s(x), 0)$. By Lemma 26.6 we have $\bot$.

  By Theorem 6 we have $\models \forall u \in El(Nat), F(u)$. Then we can conclude.
- We construct $P' \in |Nat| \to Prop$ defined by: $P'(x) := E(x,x) \wedge P(el_{Nat}(x))$.
  - $E(0,0)$ and $P(el_{Nat}(0))$ so we have $P'(0)$.
  - If $P'(x)$ then $E(x,x)$ and $P(el_{Nat}(x))$. Hence $P(S(el_{Nat}(x)))$. We also have $|S(el_{Nat}(x)) =_{El(Nat)} el_{Nat}(s(x))|$. Hence $E(s(x), s(x))$ and $P(el_{Nat}(s(x)))$. Therefore $P'(s(x))$.

  By Lemma 26.5, $\models \forall x \in \mathbb{N}, E(x,x) \Rightarrow P'(x)$. Hence $\models \forall x \in Nat, P(el_{Nat}(x))$. By Theorem 6 we have $\models \forall u \in El(Nat), P(u)$.

□

B Comparing with other categories

B.1 Variant with strict morphisms

In this subsection we are going to wonder what happens if we had a condition of strictness on the morphisms.

First we define some kind of Klop construction to our framework:

Definition 32 (Definition of the Klop Construction) Assume X is an effective set, $u \in |El(X)|$ and $F \in Prop$. We write $[u \mid F] \in |El(X)|$ defined by: $[u \mid F](x) := \; u(x) \wedge F$

Lemma 30 (Properties of the Klop Construction) *Assume X is an effective set. Then:*

$$\vDash \forall u, v \in |El(X)|, F \in Prop, |u =_{El(X)} [v \mid F]| \Leftrightarrow (|u =_{El(X)} v| \wedge F)$$

Proof:

- If $|u =_{El(X)} [v \mid F]|$: Then, there exists $x \in |X|$ such that $u(x)$. Hence, we have $[v \mid F](x)$. Therefore F. We also have $|u =_{El(X)} u|$. If $u(y)$ then $[v \mid F](y)$, so $v(y)$. If $v(y)$ then $[v \mid F](y)$, so $u(y)$. Therefore $|u =_{El(X)} v|$.
- If $|u =_{El(X)} v|$ and F: Then $|u =_{El(X)} u|$. If $u(x)$ then $v(x)$, so $[v \mid F](x)$. If $[v \mid F](x)$ then $v(x)$, so $u(x)$. Therefore $|u =_{El(X)} [u \mid F]|$.

□

Definition 33 (Definition of C_{strict}) We defined the category C_{strict} as follows:

- The objects of C_{strict} are the effective sets.
- The morphisms from X to Y in C_{strict} are the $f : El(X) \to El(Y)$ (modulo $\approx$) such that:

$$\vDash \forall u \in |El(X)|, |f(u) =_{El(Y)} f(u)| \Rightarrow |u =_{El(X)} u|$$

- The composition is the usual composition

C_{strict} is indeed a category.

We write:

- $F(X) := \; G(X) := \; X$
- $F(f)(u) := \; [f(u)||u =_{El(X)} u|]$
- $G(f) := \; f$

Lemma 31 (Properties of F and G)

- *For all $f : El(X) \to El(Y)$, $\vDash \forall u \in El(X), |(Ff)(u) = f(u)|$*
- *F is a functor from $\boldsymbol{C}$ to C_{strict}*
- *G is a functor from C_{strict} to $\boldsymbol{C}$*
- *$G \circ F = Id_C$ and $F \circ G = Id_{C_{strict}}$*

Proof:

The first point is a corollary of Lemma 30. Then the other points are trivial.

□

Theorem 32 *$\boldsymbol{C}$ and C_{strict} are isomorph, hence equivalent.*

Proof:

Corollary of Lemma 31.

□

So having strict morphisms does not change the power of the effective topos. It is just more complicated to use.

B.2 The usual effective topos

Definition 34 (Definition of C_{usual}) We write C_{usual} the usual definition of the effective topos which is the following:

- The objects of C_{usual} are the effective sets.
- The morphisms from X to Y in C_{usual} are the $F \in (|X| \times |Y|) \to Prop$ such that:
  - $\models \forall x \in |X|, y \in |Y|, F(x,y) \Rightarrow (|x =_X x| \wedge |y =_Y y|)$
  - $\models \forall x, x' \in |X|, y, y' \in |Y|, F(x,y) \Rightarrow |x =_X x'| \Rightarrow |y =_Y y'| \Rightarrow F(x', y')$
  - $\models \forall x, x' \in |X|, y, y' \in |Y|, F(x,y) \Rightarrow F(x', y') \Rightarrow |x =_X x'| \Rightarrow |y =_Y y'|$
  - $\models \forall x \in |X|, |x =_X x| \Rightarrow \exists y \in |Y|, F(x,y)$

  Modulo the relation $\approx$ defined by:
  $$F \approx G := \ (\models \forall x \in |X|, y \in |Y|, F(x,y) \Leftrightarrow G(x,y))$$
- If $F \in (|X| \times |Y|) \to Prop$ and $G \in (|Y| \times |Z|) \to Prop$ then $G \circ F \in (|X| \times |Z|) \to Prop$ is defined as follows:
  $$(G \circ F)(x,z) := \ \exists y \in |Y|, F(x,y) \wedge G(y,z)$$
  This notion of composition is coherent with $\approx$.

We write:

- $\Phi(X) := \ \Psi(X) := \ X$
- $\Phi(f)(x,y) := \ |f(el_X(x)) =_{El(Y)} el_Y(y)|$
- $\Psi(F)(u)(y) := \ \exists x \in |X|, |u =_{El(X)} el_X(x)| \wedge F(x,y)$

Lemma 33 (Properties of C_{usual})

- *Φ is a functor from C_{strict} to C_{usual}.*
- *Ψ is a functor from C_{usual} to C_{strict}.*
- *$\Psi \circ \Phi = Id_{C_{strict}}$ and $\Phi \circ \Psi = Id_{C_{usual}}$.*

Proof:
Straightforward. In particular, we use the strictness of f to prove the strictness of $\Phi(f)$.

□

Theorem 34 *$\boldsymbol{C}$ and C_{usual} are isomorph, hence they are equivalent.*

Proof:
By Lemma 33, C_{strict} and C_{usual} isomorph. By Theorem 32, $\mathbf{C}$ and C_{strict} isomorph. Therefore $\mathbf{C}$ and C_{usual} isomorph.

□

This legitimates the fact that we call C, the category we constructed, by the name of "effective topos".

B.3 Naive variant

The category C_{naive} is the naive definition of **C** without using the high level tools ($El(X)$, etc ...).

Definition 35 (Definition of C_{naive}) We define the category C_{naive} as follows:

- The objects of C_{naive} are the effective sets.
- The morphisms from X to Y in C_{naive} are the $f : X \to Y$ (modulo $\approx$).
- The composition is the usual composition.

C_{naive} is indeed a category.

With C_{naive}, we can adapt most of the work we have done in part 3 with **C**. Except that we cannot prove the axiom of unique choice. Hence, C_{naive} is not a topos and it would have been a bad choice to choose it to base our framework on it.

Of course **C** is not equivalent to C_{naive}.